ATTACHMENTS

In accordance with State Procurement Regulations:

ATTACHMENT A is the State's contract. It is provided with the RFP for informational purposes and is not required at proposal submission time. However, it must be completed, signed and returned by the selected Offeror to the Procurement Officer upon notification of proposed contract award.

ATTACHMENT B – Bid/Proposal Affidavit. This form must be completed and submitted with the Offeror's technical proposal.

ATTACHMENT C – Contract Affidavit. IT is not required at proposals submission time. It must be submitted by the selected Offeror to the Procurement Officer within 5 working days of notification of proposed award.

ATTACHMENT D – Minority Business Enterprise Participation

ATTACHMENT D-1 – MBE Utilization and Fair Solicitation Affidavit. This form must be submitted with the Offeror's technical proposal.

ATTACHMENTS D-2, D-3, and D-4 – Other MBE forms. These must be submitted to the Procurement Officer by the selected Offeror within 10 working days of notification of proposed contract award.

ATTACHMENTS D-5 and D-6 – Other MBE forms. These are submitted monthly.

ATTACHMENT E – Confidentiality and Non-Disclosure Agreement.

ATTACHMENT F – Information Technology Security Policy and Standards.

ATTACHMENT G – NAIC 120-1 MODEL COB CONTRACT PROVISIONS.

~~**ATTACHMENT H – 100-Character File Layout.** Attachment deleted~~

ATTACHMENT I – COT/GAD X-10 EFT Registration Request Form.

ATTACHMENT J-1 – Utilization Report Instructions.

ATTACHMENT J-1a – Utilization and Cost Schedule.

ATTACHMENT J-1b – Membership Analysis.

ATTACHMENT J-1c – DPPO Network Utilization**.**

ATTACHMENT N – Dental Payment Procedures.

THE BALANCE OF THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT A

DENTAL BENEFITS INSURANCE CONTRACT

THIS CONTRACT is made this _____day of _____, 2004 by and between _____ and the State of Maryland, acting through the Department of Budget and Management.

IN CONSIDERATION of the premises and the covenants herein contained, the parties agree as follows:

1. Definitions

In this Contract, the following words have the meanings indicated:

1.1 "Contract" means this Contract for Dental Benefits Insurance Services.

1.2 "Contractor" means _____ whose principal business address is _____.

1.3 "Department" means the Maryland Department of Budget and Management.

1.4 "Financial Proposal" means the Contractor's Financial Proposal dated _____.

1.5 "Procurement Officer" means _____ of the Department.

1.6 "RFP" means the Request for Proposals for _____, No. F10R4200129, dated March 16, 2004.

1.7 "State" means the State of Maryland.

1.8 "Technical Proposal" means the Contractor's Technical Proposal, dated _____.

2. Scope of Work

2.1 The Contractor shall provide dental administrative and provider network management services for eligible participants. These services shall be provided in accordance with this Contract and the following exhibits, which are attached and incorporated herein by reference:

Exhibit A - The RFP, including attachments and Excel worksheets.

Exhibit B - The Technical Proposal.

Exhibit C - The Financial Proposal.

Exhibit D – State Contract Affidavit Addendum.

2.2 If there are any inconsistencies between this Contract and Exhibits A, B, and C, the terms of this Contract shall control. If there is any conflict among the Exhibits, Exhibit A shall control.

2.3 The Procurement Officer may, at any time, by written order, make changes in the work within the general scope of the Contract. No other order, statement or conduct of the Procurement Officer or any other person shall be treated as a change or entitle the Contractor to an equitable adjustment under this section. Except as otherwise provided in this Contract, if any change under this section causes an increase or decrease in the Contractor's cost of, or the time required for, the performance of any part of the work, whether or not changed by the order, an equitable adjustment in the Contract price shall be made and the Contract modified in writing accordingly. The Contractor must assert in writing its right to an adjustment under this section within thirty (30) days of receipt of written change order and shall include a written statement setting forth the nature and cost of such claim. No claim by the Contractor shall be allowed if asserted after final payment under this Contract. Failure to agree to an adjustment under this section shall be a dispute under Article 13, Disputes. Nothing in this section shall excuse the Contractor from proceeding with the Contract as changed.

3. Time for Performance

The Contractor shall begin providing services under this Contract upon the later of execution by the Department or August 1, 2004. Unless terminated earlier as provided in this Contract, the Contractor shall provide dental benefits insurance services through December 31, 2007. The State shall have the right to exercise, at its sole option, two (2) additional one year options to extend the term of the contract.

4. Consideration and Payment

4.1 In consideration of the satisfactory performance of the work set forth in this Contract, the Department shall pay the Contractor a sum not to exceed the rates established in Exhibit C, Contractor's Financial Proposal.

4.2 Each invoice must reflect the Contractor's federal tax identification number, which is _____. Payments to the Contractor pursuant to this Contract shall be made no later than 30 days after the State's receipt of a proper invoice from the Contractor. Charges for late payment of invoices, other than as prescribed by Title 15, Subtitle 1, of the State Finance and Procurement Article, Annotated Code of Maryland, as from time to time amended, are prohibited. The final payment under this Contract will not be made until after certification is received from the Comptroller of the State that all taxes have been paid. Electronic funds transfer will be used by the State to pay the Contractor for this contract and any other State payments due Contractor unless the State's Comptroller's Office grants the Contractor an exemption.

4.3 In addition to any other available remedies if, in the opinion of the Procurement Officer, the Contractor fails to perform in a satisfactory and timely manner, the Procurement Officer may refuse or limit approval of any invoice for payment, and may cause payments to the Contractor to be reduced or withheld until such time as the Contractor meets performance standards as established by the Procurement Officer pursuant to this Contract.

5. Personnel

Contractor agrees that all personnel identified in its proposal shall be assigned to the State account for the term of the Contract, including any extension, unless such personnel are no longer employed by the Contractor.

6. Rights to Records

6.1 The Contractor agrees that all documents and materials, including but not limited to, reports, drawings, studies, specifications, estimates, tests, maps, photographs, designs, graphics, mechanical, artwork, computations and data prepared by the Contractor for purposes of this Contract shall be the sole property of the Department and shall be available to the Department at any time. The Department shall have the right to use the same without restriction and without compensation to the Contractor other than that specifically provided by this Contract.

6.2 The Contractor agrees that at all times during the term of this Contract and thereafter, the works created and services performed under this Contract shall be "works made for hire" as that term is interpreted under U.S. copyright law. To the extent that any products created under this Contract are not works for hire for the Department, the Contractor hereby relinquishes, transfers, and assigns to the State all of its rights, title, and interest (including all intellectual property rights) to all such products created under this Contract, and will cooperate reasonably with the State in effectuating and registering any necessary assignments.

6.3 The Contractor shall report to the Department, promptly and in written detail, each notice or claim of copyright infringement received by the Contractor with respect to all data delivered under this Contract.

6.4 The Contractor shall not affix any restrictive markings upon any data and if such markings are affixed, the Department shall have the right at any time to modify, remove, obliterate, or ignore such warnings.

6.5 Upon termination of this Contract, the Contractor, at its own expense, shall deliver any equipment, software or other property provided by the State to the place designated by the Procurement Officer.

6.6 Nothing in this Section 6 shall abrogate or transfer any intellectual property rights of the Contractor in its proprietary information related to its methodologies, methods of analysis, ideas, know how, methods, techniques, and skills possessed prior to this Contract.

7. Confidentiality

Subject to the Maryland Public Information Act and any other applicable laws, all confidential or proprietary information and documentation relating to either party (including without limitation, any information or data stored within the Contractor's computer systems) shall be held in absolute confidence by the other party. Each party shall, however, be permitted to disclose relevant confidential information to its officers, agents and employees to the extent that such disclosure is necessary for the performance of their duties under this Contract, provided the data may be collected, used, disclosed, stored and disseminated only as provided by and consistent with the law. The provisions of this section shall not apply to information that (a) is lawfully in the public domain; (b) has been independently developed by the other party without violation of this Contract; (c) was already in the possession of such party, (d) was supplied to such party by a third party lawfully in possession thereof and legally permitted to further disclose the information or (e) which such party is required to disclose by law.

8. Non-Hiring of Employees

No official or employee of the State of Maryland as defined under State Government Article section 15-102, Annotated Code of Maryland, whose duties as such official or employee include matters relating to or affecting the subject matter of this Contract shall, during the pendancy and term of this Contract and while serving as an official or employee of the State become or be an employee of the Contractor or any entity that is a subcontractor on this Contract.

9. Disputes

This Contract shall be subject to the provisions of Title 15, Subtitle 2, of the State Finance and Procurement Article of the Annotated Code of Maryland, as from time to time amended, and COMAR 21.10 (Administrative and Civil Remedies). Pending resolution of a claim, the Contractor shall proceed diligently with the performance of the Contract in accordance with the Procurement Officer's decision. Unless a lesser period is provided by applicable statute, regulation, or the Contract, the Contractor must file a written notice of claim with the Procurement Officer within 30 days after the basis for the claim is known or should have been known, whichever is earlier. Contemporaneously with or within 30 days of the filing of a notice of claim, but no later than the date of final payment under the Contract, the Contractor must submit to the Procurement Officer its written claim containing the information specified in COMAR 21.10.04.02.

10. Maryland Law

This Contract shall be construed, interpreted, and enforced according to the laws of the State of Maryland.

11. Nondiscrimination in Employment

The Contractor agrees: (a) not to discriminate in any manner against an employee or applicant for employment because of race, color, religion, creed, age, sex, marital status, national origin, ancestry, or disability of a qualified individual with a disability; (b) to include a provision similar to that contained in subsection (a), above, in any subcontract except a subcontract for standard commercial supplies or raw materials; and (c) to post and to cause subcontractors to post in conspicuous places available to employees and applicants for employment, notices setting forth the substance of this clause.

12. Contingent Fee Prohibition

The Contractor warrants that it has not employed or retained any person, partnership, corporation, or other entity, other than a bona fide employee, bona fide agent, bona fide salesperson, or commercial selling agency working for the Contractor to solicit or secure this Contract, and that it has not paid or agreed to pay any person, partnership, corporation or other entity, other than a bona fide employee, bona fide salesperson or commercial selling agency, any fee or other consideration contingent on the making of this Contract.

13. Nonavailability of Funding

If the General Assembly fails to appropriate funds or if funds are not otherwise made available for continued performance for any fiscal period of this Contract succeeding the first fiscal period, this Contract shall be canceled automatically as of the beginning of the fiscal year for which funds were not appropriated or otherwise made available; provided, however, that this will not affect either the State's rights or the Contractor's rights under any termination clause in this Contract. The effect of termination of the Contract hereunder will be to discharge both the Contractor and the State from future performance of the Contract, but not from their rights and obligations existing at the time of termination. The Contractor shall be reimbursed for the reasonable value of any nonrecurring costs incurred but not amortized in the price of the Contract. The State shall notify the Contractor as soon as it has knowledge that funds may not be available for the continuation of this Contract for each succeeding fiscal period beyond the first.

14. Termination for Cause

If the Contractor fails to fulfill its obligations under this Contract properly and on time, or otherwise violates any provision of the Contract, the State may terminate the Contract by written notice to the Contractor. The notice shall specify the acts or omissions relied upon as cause for termination. All finished or unfinished work provided by the Contractor shall, at the State's option, become the State's property. The State of Maryland shall pay the Contractor fair and equitable compensation for satisfactory performance prior to receipt of notice of termination, less the amount of damages caused by the Contractor's breach. If the damages are more than the compensation payable to the Contractor, the Contractor will remain liable after termination and the State can affirmatively collect damages. Termination hereunder, including the termination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.11B.

15. Termination for Convenience

The performance of work under this Contract may be terminated by the State in accordance with this clause in whole, or from time to time in part, whenever the State shall determine that such termination is in the best interest of the State. The State will pay all reasonable costs associated with this Contract that the Contractor has incurred up to the date of termination, and all reasonable costs associated with termination of the Contract; provided, however, the Contractor shall not be reimbursed for any anticipatory profits that have not been earned up to the date of termination. Termination hereunder, including the determination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.12 (A)(2).

16. Delays and Extensions of Time

The Contractor agrees to perform the work under this Contract continuously and diligently. No charges or claims for damages shall be made by the Contractor for any delays or hindrances from any cause whatsoever during the progress of any portion of the work specified in this Contract. Time extensions will be granted only for excusable delays that arise from unforeseeable causes beyond the control and without the fault or negligence of the Contractor, including but not restricted to acts of God, acts of the public enemy, acts of the State in either its sovereign or contractual capacity, acts of another contractor in the performance of a contract with the State, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, or delays of subcontractors or suppliers arising from unforeseeable causes beyond the control and without the fault or negligence of either the Contractor or the subcontractors or suppliers.

17. Suspension of Work

The State unilaterally may order the Contractor in writing to suspend, delay, or interrupt all or any part of its performance for such period of time as the Procurement Officer may determine to be appropriate for the convenience of the State.

18. Pre-Existing Regulations

In accordance with the provisions of Section 11-206 of the State Finance and Procurement Article, Annotated Code of Maryland, as from time to time amended, the regulations set forth in Title 21 of the Code of Maryland Regulations (COMAR 21) in effect on the date of execution of this Contract are applicable to this Contract.

19. Financial Disclosure

The Contractor shall comply with the provisions of Section 13-221 of the State Finance and Procurement Article of the Annotated Code of Maryland, as from time to time amended, which requires that every business that enters into contracts, leases, or other agreement with the State of Maryland or its agencies during a calendar year under which the business is to receive in the aggregate $100,000 or more, shall within 30 days of the time when the aggregate value of these contracts, leases or other agreements reaches $100,000, file with the Secretary of the State of Maryland certain specified information to include disclosure of beneficial ownership of the business.

20. Political Contribution Disclosure

The Contractor shall comply with the Election Law Article, Sections 14-101 through 14-108, of the Annotated Code of Maryland, which requires that every person that enters into contracts, leases, or other agreements with the State, a county or an incorporated municipality or their agencies, during a calendar year under which the person receives in the aggregate $100,000 or more, shall file with the State Board of Elections a statement disclosing contributions in excess of $500 made during the reporting period to a candidate for elective office in any primary or general election. The statement shall be filed with the State Board of Elections: (1) before a purchase or execution of a lease or contract by the State, a county, an incorporated municipality, or their agencies, and shall cover the preceding two calendar years; and (2) if the contribution is made after the execution of a lease or contract, then twice a year, throughout the contract term, on: (a) February 5, to cover the 6-month period ending January 31; and (b) August 5, to cover the 6-month period ending July 31.

21. Retention of Records

The Contractor shall retain and maintain all records and documents in any way relating to this Contract for three years after final payment by the State of Maryland under this Contract or any applicable statute of limitations, whichever is longer, and shall make them available for inspection and audit by authorized representatives of the State, including the Procurement Officer or the Procurement Officer's designee, at all reasonable times. All records related in any way to the Contract are to be retained for the entire time provided under this section.

22. Compliance with Laws

The Contractor hereby represents and warrants that:

A. It is qualified to do business in the State of Maryland and that it will take such action as, from time to time hereafter, may be necessary to remain so qualified;

B. It is not in arrears with respect to the payment of any monies due and owing the State of Maryland, or any department or unit thereof, including but not limited to the payment of taxes and employee benefits, and that it shall not become so in arrears during the term of this Contract;

C. It shall comply with all federal, State and local laws, regulations, and ordinances applicable to its activities and obligations under this Contract; and,

D. It shall obtain, at its expense, all licenses, permits, insurance, and governmental approvals, if any, necessary to the performance of its obligations under this Contract.

23. Cost and Price Certification

By submitting cost or price information, the Contractor certifies to the best of its knowledge that the information submitted is accurate, complete, and current as of a mutually determined specified date prior to the conclusion of any price discussions or negotiations.

The price under this Contract and any change order or modification hereunder, including profit or fee, shall be adjusted to exclude any significant price increases occurring because the Contractor furnished cost or price information which, as of the date agreed upon by the parties, was inaccurate, incomplete, or not current.

24. Subcontracting; Assignment

The Contractor may not subcontract any portion of the services provided under this Contract without obtaining the prior written approval of the State of Maryland, nor may the Contractor assign this Contract or any of its rights or obligations hereunder, without the prior written approval of the State. Any such subcontract or assignment shall include the terms of sections 8, and 10 through 23 of this Contract and any other terms and conditions that the State deems necessary to protect its interests. The State shall not be responsible for the fulfillment of the Contractor's obligations to the subcontractors.

25. Indemnification

25.1 The Contractor shall indemnify the State against liability for any costs, expenses, loss, suits, actions, or claims of any character arising from or relating to the performance of the Contractor or its subcontractors under this Contract.

25.2 The State of Maryland has no obligation to provide legal counsel or defense to the Contractor or its subcontractors in the event that a suit, claim or action of any character is brought by any person not party to this Contract against the Contractor or its subcontractors as a result of or relating to the Contractor's obligations under this Contract.

25.3 The State has no obligation for the payment of any judgments or the settlement of any claims against the Contractor or its subcontractors as a result of or relating to the Contractor's obligations under this Contract.

25.4 The Contractor shall immediately notify the Procurement Officer of any claim or suit made or filed against the Contractor or its subcontractors regarding any matter resulting from or relating to the Contractor's obligations under the Contract, and will cooperate, assist, and consult with the State in the defense or investigation of any claim, suit, or action made or filed against the State as a result of or relating to the Contractor's performance under this Contract.

26. Administrative

26.1 **Procurement Officer**. The work to be accomplished under this Contract shall be performed under the direction of the Procurement Officer. All matters relating to the interpretation of this Contract shall be referred to the Procurement Officer for determination.

26.2 **Notices**. All notices hereunder shall be in writing and either delivered personally or sent by certified or registered mail, postage prepaid as follows:

If to the State:

If to the Contractor:

IN WITNESS THEREOF, the parties have executed this Contract as of the date hereinabove set forth.

CONTRACTOR	MARYLAND DEPARTMENT OF BUDGET AND MANAGEMENT
_____	_____
By:	By: James C. DiPaula, Secretary
_____	_____
Date	Date
_____	_____
Witness	Witness

Approved for form and legal
sufficiency this _____ day
of _____ 2004.

_____

Assistant Attorney General

APPROVED BY BPW: _____ _____
(Date) (BPW Item #)

ATTACHMENT B

BID/PROPOSAL AFFIDAVIT
COMAR 21.05.08.07

BID/PROPOSAL AFFIDAVIT

A. AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the (title) _____ and the duly authorized representative of (business) _____ and that I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

B. AFFIRMATION REGARDING BRIBERY CONVICTIONS

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business (as is defined in Section 16-101(b) of the State Finance and Procurement Article of the Annotated Code of Maryland), or any of its officers, directors, partners, or any of its employees directly involved in obtaining or performing contracts with public bodies (as is defined in Section 16-101(f) of the State Finance and Procurement Article of the Annotated Code of Maryland), has been convicted of, or has had probation before judgment imposed pursuant to Criminal Procedure Article, §6-220, Annotated Code of Maryland, or has pleaded nolo contendere to a charge of, bribery, attempted bribery, or conspiracy to bribe in violation of Maryland law, or of the law of any other state or federal law, except as follows (indicate the reasons why the affirmation cannot be given and list any conviction, plea, or imposition of probation before judgment with the date, court, official or administrative body, the sentence or disposition, the name(s) of person(s) involved, and their current positions and responsibilities with the business):

_____
_____
_____.

C. AFFIRMATION REGARDING OTHER CONVICTIONS

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business, or any of its officers, directors, partners, or any of its employees directly involved in obtaining or performing contracts with public bodies, has:

(a) Been convicted under state or federal statute of a criminal offense incident to obtaining, attempting to obtain, or performing a public or private contract, fraud, embezzlement, theft, forgery, falsification or destruction of records, or receiving stolen property;

(b) Been convicted of any criminal violation of a state or federal antitrust statute;

(c) Been convicted under the provisions of Title 18 of the United States Code for violation of the Racketeer Influenced and Corrupt Organization Act, 18 U.S.C. §1961, et seq., or the Mail Fraud Act, 18 U.S.C. §1341, et seq., for acts arising out of the submission of bids or proposals for a public or private contract;

(d) Been convicted of a violation of the State Minority Business Enterprise Law, Section 14-308 of the State Finance and Procurement Article of the Annotated Code of Maryland;

(e) Been convicted of conspiracy to commit any act or omission that would constitute grounds for conviction or liability under any law or statute described in subsection (a), (b), (c), or (d) above;

(f) Been found civilly liable under a state or federal antitrust statute for acts or omissions in connection with the submission of bids or proposals for a public or private contract;

(g) Admitted in writing or under oath, during the course of an official investigation or other proceedings, acts or omissions that would constitute grounds for conviction or liability under any law or statute described above, except as follows (indicate reasons why the affirmations cannot be given, and list any conviction, plea, or imposition of probation before judgment with the date, court, official or administrative body, the sentence or disposition, the name(s) of the person(s) involved and their current positions and responsibilities with the business, and the status of any debarment):

_____
_____
_____.

D. AFFIRMATION REGARDING DEBARMENT

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business, or any of its officers, directors, partners, or any of its employees directly involved in obtaining or performing contracts with public bodies, has ever been suspended or debarred (including being issued a limited denial of participation) by any public entity, except as follows (list each debarment or suspension providing the dates of the suspension or debarment, the name of the public entity and the status of the proceedings, the name(s) of the person(s) involved and their current positions and responsibilities with the business, the grounds of the debarment or suspension, and the details of each person's involvement in any activity that formed the grounds of the debarment or suspension):

_____
_____
_____.

E. AFFIRMATION REGARDING DEBARMENT OF RELATED ENTITIES

I FURTHER AFFIRM THAT:

(1) The business was not established and it does not operate in a manner designed to evade the application of or defeat the purpose of debarment pursuant to Sections 16-101, et seq., of the State Finance and Procurement Article of the Annotated Code of Maryland; and

(2) The business is not a successor, assignee, subsidiary, or affiliate of a suspended or debarred business, except as follows (you must indicate the reasons why the affirmations cannot be given without qualification):

_____
_____
_____.

F. SUB-CONTRACT AFFIRMATION

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business, has knowingly entered into a contract with a public body under which a person debarred or suspended under Title 16 of the State Finance and Procurement Article of the Annotated Code of Maryland will provide, directly or indirectly, supplies, services, architectural services, construction related services, leases of real property, or construction.

G. AFFIRMATION REGARDING COLLUSION

I FURTHER AFFIRM THAT:

Neither I, nor to the best of my knowledge, information, and belief, the above business has:

(1) Agreed, conspired, connived, or colluded to produce a deceptive show of competition in the compilation of the accompanying bid or offer that is being submitted;

(2) In any manner, directly or indirectly, entered into any agreement of any kind to fix the bid price or price proposal of the bidder or offeror or of any competitor, or otherwise taken any action in restraint of free competitive bidding in connection with the contract for which the accompanying bid or offer is submitted.

H. FINANCIAL DISCLOSURE AFFIRMATION

I FURTHER AFFIRM THAT:

I am aware of, and the above business will comply with, the provisions of Section 13-221 of the State Finance and Procurement Article of the Annotated Code of Maryland, which require that every business that enters into contracts, leases, or other agreements with the State of Maryland or its agencies during a calendar year under which the business is to receive in the aggregate $100,000 or more shall, within 30 days of the time when the aggregate value of the contracts, leases, or other agreements reaches $100,000, file with the Secretary of State of Maryland certain specified information to include disclosure of beneficial ownership of the business.

I. POLITICAL CONTRIBUTION DISCLOSURE AFFIRMATION

I FURTHER AFFIRM THAT:

I am aware of, and the above business will comply with, Election Law Article, §§14-101—14-108, Annotated Code of Maryland, which requires that every person that enters into contracts, leases, or other agreements with the State of Maryland, including its agencies or a political subdivision of the State, during a calendar year in which the person receives in the aggregate $100,000 or more shall file with the State Administrative Board of Election Laws a statement disclosing contributions in excess of $500 made during the reporting period to a candidate for elective office in any primary or general election.

J. DRUG AND ALCOHOL FREE WORKPLACE

(Applicable to all contracts unless the contract is for a law enforcement agency and the agency head or the agency head's designee has determined that application of COMAR 21.11.08 and this certification would be inappropriate in connection with the law enforcement agency's undercover operations.)

I CERTIFY THAT:

(1) Terms defined in COMAR 21.11.08 shall have the same meanings when used in this certification.

(2) By submission of its bid or offer, the business, if other than an individual, certifies and agrees that, with respect to its employees to be employed under a contract resulting from this solicitation, the business shall:

(a) Maintain a workplace free of drug and alcohol abuse during the term of the contract;

(b) Publish a statement notifying its employees that the unlawful manufacture, distribution, dispensing, possession, or use of drugs, and the abuse of drugs or alcohol is prohibited in the business' workplace and specifying the actions that will be taken against employees for violation of these prohibitions;

(c) Prohibit its employees from working under the influence of drugs or alcohol;

(d) Not hire or assign to work on the contract anyone whom the business knows, or in the exercise of due diligence should know, currently abuses drugs or alcohol and is not actively engaged in a bona fide drug or alcohol abuse assistance or rehabilitation program;

(e) Promptly inform the appropriate law enforcement agency of every drug-related crime that occurs in its workplace if the business has observed the violation or otherwise has reliable information that a violation has occurred;

(f) Establish drug and alcohol abuse awareness programs to inform its employees about:

(i) The dangers of drug and alcohol abuse in the workplace;

(ii) The business' policy of maintaining a drug and alcohol free workplace;

(iii) Any available drug and alcohol counseling, rehabilitation, and employee assistance programs; and

(iv) The penalties that may be imposed upon employees who abuse drugs and alcohol in the workplace;

(g) Provide all employees engaged in the performance of the contract with a copy of the statement required by §J(2)(b), above;

(h) Notify its employees in the statement required by §J(2)(b), above, that as a condition of continued employment on the contract, the employee shall:

(i) Abide by the terms of the statement; and

(ii) Notify the employer of any criminal drug or alcohol abuse conviction for an offense occurring in the workplace not later than 5 days after a conviction;

(i) Notify the procurement officer within 10 days after receiving notice under §J(2)(h)(ii), above, or otherwise receiving actual notice of a conviction;

(j) Within 30 days after receiving notice under §J(2)(h)(ii), above, or otherwise receiving actual notice of a conviction, impose either of the following sanctions or remedial measures on any employee who is convicted of a drug or alcohol abuse offense occurring in the workplace:

(i) Take appropriate personnel action against an employee, up to and including termination; or

(ii) Require an employee to satisfactorily participate in a bona fide drug or alcohol abuse assistance or rehabilitation program; and

(k) Make a good faith effort to maintain a drug and alcohol free workplace through implementation of §J(2)(a)—(j), above.

(3) If the business is an individual, the individual shall certify and agree as set forth in §J(4), below, that the individual shall not engage in the unlawful manufacture, distribution, dispensing, possession, or use of drugs or the abuse of drugs or alcohol in the performance of the contract.

(4) I acknowledge and agree that:

(a) The award of the contract is conditional upon compliance with COMAR 21.11.08 and this certification;

(b) The violation of the provisions of COMAR 21.11.08 or this certification shall be cause to suspend payments under, or terminate the contract for default under COMAR 21.07.01.11 or 21.07.03.15, as applicable; and

(c) The violation of the provisions of COMAR 21.11.08 or this certification in connection with the contract may, in the exercise of the discretion of the Board of Public Works, result in suspension and debarment of the business under COMAR 21.08.06.

K. CERTIFICATION OF CORPORATION REGISTRATION AND TAX PAYMENT

I FURTHER AFFIRM THAT:

(1) The business named above is a (domestic ___) (foreign __) corporation registered in accordance with the Corporations and Associations Article, Annotated Code of Maryland, and that it is in good standing and has filed all of its annual reports, together with filing fees, with the Maryland State Department of Assessments and Taxation, and that the name and address of its resident agent filed with the State Department of Assessments and Taxation is: Name: Address: __ .

(If not applicable, so state).

(2) Except as validly contested, the business has paid, or has arranged for payment of, all taxes due the State of Maryland and has filed all required returns and reports with the Comptroller of the Treasury, the State Department of Assessments and Taxation, and the Department of Labor, Licensing, and Regulation, as applicable, and will have paid all withholding taxes due the State of Maryland prior to final settlement.

L. CONTINGENT FEES

I FURTHER AFFIRM THAT:

The business has not employed or retained any person, partnership, corporation, or other entity, other than a bona fide employee or agent working for the business, to solicit or secure the Contract, and that the business has not paid or agreed to pay any person, partnership, corporation, or other entity, other than a bona fide employee or agent, any fee or any other consideration contingent on the making of the Contract.

M. ACKNOWLEDGEMENT

I ACKNOWLEDGE THAT this Affidavit is to be furnished to the Procurement Officer and may be distributed to units of: (1) the State of Maryland; (2) counties or other subdivisions of the State of Maryland; (3) other states; and (4) the federal government. I further acknowledge that this Affidavit is subject to applicable laws of the United States and the State of Maryland, both criminal and civil, and that nothing in this Affidavit or any contract resulting from the submission of this bid or proposal shall be construed to supersede, amend, modify or waive, on behalf of the State of Maryland, or any unit of the State of Maryland having jurisdiction, the exercise of any statutory right or remedy conferred by the Constitution and the laws of Maryland with respect to any misrepresentation made or any violation of the obligations, terms and convenants undertaken by the above business with respect to (1) this Affidavit, (2) the contract, and (3) other Affidavits comprising part of the contract.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____ By:

_____

Authorized Representative and Affiant

ATTACHMENT C

COMAR 21.07.01.25
CONTRACT AFFIDAVIT

A. AUTHORIZED REPRESENTATIVE

I HEREBY AFFIRM THAT:

I am the _____(title)_____ and the duly authorized representative of _____(business)_____ and that I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

B. CERTIFICATION OF CORPORATION REGISTRATION AND TAX PAYMENT

I FURTHER AFFIRM THAT:

(1) The business named above is a (domestic___) (foreign____) corporation registered in accordance with the Corporations and Associations Article, Annotated Code of Maryland, and that it is in good standing and has filed all of its annual reports, together with filing fees, with the Maryland State Department of Assessments and Taxation, and that the name and address of its resident agent filed with the State Department of Assessments and Taxation is: Name:_____ Address:_____.

(2) Except as validly contested, the business has paid, or has arranged for payment of, all taxes due the State of Maryland and has filed all required returns and reports with the Comptroller of the Treasury, the State Department of Assessments and Taxation, and the Department of Labor, Licensing, and Regulation, as applicable, and will have paid all withholding taxes due the State of Maryland prior to final settlement.

C. CERTAIN AFFIRMATIONS VALID

I FURTHER AFFIRM THAT:

To the best of my knowledge, information, and belief, each of the affirmations, certifications, or acknowledgements contained in that certain Bid/Proposal Affidavit dated _____ , 2004 , and executed by me for the purpose of obtaining the contract to which this Exhibit is attached remains true and correct in all respects as if made as of the date of this Contract Affidavit and as if fully set forth herein.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date:_____ By:_____

(Authorized Representative and Affiant)

ATTACHMENT D

STATE OF MARYLAND

Department of Budget & Management

MINORITY BUSINESS ENTERPRISE PARTICIPATION

PURPOSE

Contractor shall structure its procedures for the performance of the work required in this contract to attempt to achieve the minority business enterprise (MBE) goal stated in the Invitation for Bids or Request for Proposals. MBE performance must be in accordance with this Exhibit, as authorized by Code of Maryland Regulations (COMAR) 21.11.03. Contractor agrees to exercise all good faith efforts to carry out the requirements set forth in this Exhibit.

DEFINITIONS

As used in this Exhibit, the following words have the meanings indicated.

- "Certification" means a determination made by the Maryland Department of Transportation that a legal entity is a minority business enterprise.
- "MBE Liaison" is the employee designated to administer this Department's MBE program.
- "Minority Business Enterprise" or "MBE" means any legal entity, other than a joint venture, organized to engage in commercial transactions, that is:

  (1) at least 51 percent owned and controlled by one or more individuals who are socially and economically disadvantaged; and
  (2) managed by, and the daily business operations of which are controlled by, one or more of the socially and economically disadvantaged individuals who own it.

Note: A minority business enterprise also includes a not-for-profit entity organized to promote the interests of physically or mentally disabled individuals.

An MBE **must be** certified in order to have its contract participation counted under the Department's MBE program.

MBE GOALS AND SUB-GOALS

- ☐ An overall MBE subcontract participation goal of one-half percent (.5%) of total premium paid has been established for this procurement.

  By submitting a response to this solicitation, the bidder or offeror agrees that these dollar amounts of the contract will be performed by certified minority business enterprises as specified.

- A prime contractor — including an MBE prime contractor — must accomplish an amount of work not less than the MBE subcontract goal with certified MBE subcontractors.
- A prime contractor comprising a joint venture that includes MBE partner(s) must accomplish the MBE subcontract goal with certified MBE subcontractors.

SOLICITATION AND CONTRACT FORMATION

- A bidder or offeror must include with its bid or offer a completed MBE Utilization and Fair Solicitation Affidavit (ATTACHMENT D-1) whereby the bidder or offeror acknowledges the certified MBE participation goal, commits to make a good faith effort to achieve the goal, and affirms that MBE subcontractors were treated fairly in the solicitation process. **If a bidder or offeror fails to submit this affidavit, the Department may deem the bid or offer non-responsive.**

- Within 10 working days from notification that it is the apparent awardee or from the date of the actual award, whichever is earlier, the apparent awardee must provide the following documentation to the MBE Liaison. **If the apparent awardee fails to return each completed document within the required time, the award is voidable**.

    (1) Outreach Efforts Compliance (ATTACHMENT D-2)
    (2) MBE Participation Schedule (ATTACHMENT D-3)
    (3) Subcontractor Project Participation Statement (ATTACHMENT D-4)
    (4) In the rare event that the apparent awardee believes a waiver is necessary of the overall MBE goal or of any sub-goal by MBE classification, it may submit a waiver request that complies with COMAR 21.11.03.11 in the place of the MBE Participation Schedule.
    (5) Any other documentation required by the Department's MBE Liaison to ascertain bidder or offeror responsibility in connection with the certified MBE participation goal.

CONTRACT ADMINISTRATION REQUIREMENTS

Contractor shall:

1. Submit monthly to the Department a report listing any unpaid invoices, over 30 days old, received from any certified MBE subcontractor, the amount of each invoice and the reason payment has not been made.

2. Include in its agreements with its certified MBE subcontractors a requirement that those subcontractors submit monthly to the Department a report that identifies the prime contract and lists all payments received from Contractor in the preceding 30 days, as well as any outstanding invoices, and the amount of those invoices.

3. Maintain such records as are necessary to confirm compliance with its MBE participation obligations. These records must indicate the identity of certified minority and non-minority subcontractors employed on the contract, the type of work performed by each, and the actual dollar value of work performed.

4. Consent to provide such documentation as reasonably requested and to provide right-of-entry at reasonable times for purposes of the State's representatives verifying compliance with the MBE participation obligations. Contractor must retain all records concerning MBE participation and make them available for State inspection for three years after final completion of the contract.

5. At the option of the procurement agency, upon completion of the contract and before final payment and/or release of retainage, submit a final report in affidavit form and under penalty of perjury, of all payments made to, or withheld from MBE subcontractors.

ADDITIONAL ATTACHMENTS TO
MINORITY BUSINESS ENTERPRISE PARTICIPATION FORMS

ATTACHMENT D-1 - Certified MBE Utilization and Fair Solicitation Affidavit (must be submitted with bid or offer)

ATTACHMENT D-2 - Outreach Efforts Compliance (must be submitted within 10 working days of notification of apparent award)

ATTACHMENT D-3 - MBE Participation Schedule (must be submitted with Attachment D-2)

ATTACHMENT D-4 - Subcontractor Project Participation Statement (must be submitted with Attachment D-2)

ATTACHMENT D-5 - Maryland Department of Budget and Management Minority Business Enterprise Participation – Prime Contractor Paid/Unpaid MBE Invoice Report

ATTACHMENT D-6 - Maryland Department of Budget and Management Minority Business Enterprise Participation – Subcontractor Payment Report

ATTACHMENT D-1

CERTIFIED MBE UTILIZATION AND FAIR SOLICITATION AFFIDAVIT

In conjunction with the bid or offer submitted in response to Solicitation No. F10R4200129, I affirm the following:

1. I acknowledge the overall certified Minority Business Enterprise (MBE) participation goal of one-half percent (.5%) of total premium paid. I commit to make a good faith effort to achieve this goal.

2. I understand that if I am notified that I am selected for contract award, I must submit the documentation described in the MBE Participation Exhibit within 10 working days of receiving notice of the potential award or from the date of actual award, whichever is earlier. If I fail to do so, I understand any apparent award will be deemed voidable.

3. In the solicitation of subcontract quotations or offers, MBE subcontractors were provided not less than the same information and amount of time to respond as were non-MBE subcontractors.

4. The solicitation process was conducted in such a manner so as to not place MBE subcontractors at a competitive disadvantage to non-MBE subcontractors.

I solemnly affirm under the penalties of perjury that the contents of this paper are true to the best of my knowledge, information, and belief.

_____ _____
Bidder/Offeror Name Signature of Affiant

_____ _____
Address Printed Name, Title

_____
Date

SUBMIT THIS AFFIDAVIT WITH BID/PROPOSAL

ATTACHMENT D-2

OUTREACH EFFORTS COMPLIANCE STATEMENT

In conjunction with the bid or offer submitted in response to Solicitation No. F10R4200129, I state the following:

1. Bidder/ Offeror identified opportunities to subcontract in these specific work categories:

2. Attached to this form are copies of written solicitations (with bidding instructions) used to solicit certified MBEs for these subcontract opportunities.

3. Bidder/Offeror made the following attempts to contact personally the solicited MBEs:

4. ☐ Bidder/Offeror assisted MBEs to fulfill or to seek waiver of bonding requirements. (DESCRIBE EFFORTS)

   ☐ This project does not involve bonding requirements.

5. ☐ Bidder/Offeror did/did not attend the pre-bid conference
   ☐ No pre-bid conference was held.

_____ By: _____

Bidder/Offeror Name

_____ _____

Address Name, Title

_____

Date

ATTACHMENT D-3

MBE PARTICIPATION SCHEDULE

Prime Contractor (Firm Name, Address, Phone)	Project Description
Project Number	Total Contract Amount $

List Information For Each Certified MBE Subcontractor On This Project

A. Minority Firm Name, Address, Phone	MBE Classification: _____ MBE Certification Number
Work To Be Performed	
Project Commitment Date	Project Completion Date
Agreed Dollar Amount	Percentage Of Total Contract
B. Minority Firm Name, Address, Phone	MBE Classification: _____ MBE Certification Number
Work To Be Performed	
Project Commitment Date	Project Completion Date
Agreed Dollar Amount	Percentage Of Total Contract
C. Minority Firm Name, Address, Phone	MBE Classification: _____ MBE Certification Number
Work To Be Performed	
Project Commitment Date	Project Completion Date
Agreed Dollar Amount	Percentage Of Total Contract
D. Minority Firm Name, Address, Phone	MBE Classification: _____ MBE Certification Number
Work To Be Performed	
Project Commitment Date	Project Completion Date
Agreed Dollar Amount	Percentage Of Total Contract

MBE Firms Total Dollar Amount Overall $_____
MBE Firms Total Percentage Overall _____%
African American MBE Dollar Amount $_____
African American MBE Percentage _____%
Women MBE Dollar Amount $_____
Women MBE Percentage _____%

List Additional MBE Subcontractors Or Provide Any Additional Comments on Separate Paper.

Document Prepared By: (please print or type)
Name:_____ Title:_____

ATTACHMENT D-4

SUBCONTRACTOR PROJECT PARTICIPATION

STATEMENT

SUBMIT ONE FORM FOR EACH CERTIFIED MBE LISTED IN THE MBE PARTICIPATION SCHEDULE

Provided that _____ is awarded the State contract in
(Prime Contractor Name)

conjunction with Solicitation No. _____, it and _____,
(Subcontractor Name)

MDOT Certification No. _____, intend to enter into a contract by which Subcontractor shall:

(describe work)_____
_____
_____
_____

☐ No bonds are required of Subcontractor

☐ The following amount and type of bonds are required of Subcontractor:

_____ _____
Prime Contractor Signature Subcontractor Signature

By:_____ By: _____
Name, Title Name, Title

_____ _____
Date Date

This form is to be completed monthly by the **prime** contractor.

ATTACHMENT D-5

Maryland Department of Budget and Management

Minority Business Enterprise Participation

Prime Contractor Paid/Unpaid MBE Invoice Report

Report #: __1___ Reporting Period (Month/Year): __/_____ **Report Due By the 15th of the following Month.**	Contract # _____ Contracting Unit _____ Contract Amount_____ MBE Sub Contract Amt._____ Contract Begin Date_____ Contract End Date_____ Services Provided_____

Prime Contractor:	Contact Person:	
Address:		
City:	State:	ZIP:
Phone:	FAX:	
Subcontractor Name:	Contact Person:	
Phone:	FAX:	
Subcontractor Services Provided:		

List all payments made to MBE subcontractor named above during this reporting period. **1.** **2.** **3.** **4.** **Total Dollars Paid: $_____**	**List dates/amounts of any unpaid invoices received from subcontractor during this reporting period.** **1.** **2.** **3.** **4.** **Total Dollars Unpaid: $_____**

**If more than one MBE subcontractor is used for this contract please use separate forms.

Return one (1) copy of this form to each of the following addresses:

Department of Budget and Management Employee Benefits Division 301 W. Preston Street, 5th Floor Baltimore, MD 21201 ATTN: Napoleon Curameng	MBE Liaison Officer Department of Budget and Management Procurement Unit, Room 109 45 Calvert Street Annapolis, MD 21401

Signature:_____ Date:_____

This form is to be completed monthly by the **MBE** contractor.

ATTACHMENT D-6

Maryland Department of Budget and Management
Minority Business Enterprise Participation
Subcontractor Paid/Unpaid MBE Invoice Report

Report _____ Month/Year _____ **Report Due By the 15th of the following Month.**	Contract # _____ Contracting Unit _____ Contract Amount_____ MBE Sub Contract Amt._____ Contract Begin Date_____ Contract End Date_____ Services Provided_____

MBE Subcontractor Name:

MDOT Certification #

Contact Person

Address:

City	State:	ZIP:

Phone:	FAX:

Subcontractor Services Provided:

List all payments received from Prime Contractor in the preceding 30 days. **1.** **2.** **3.** **Total Dollars Paid: $_____**	**List dates and amounts of any outstanding invoices.** **1.** **2.** **3.** **Total Dollars Unpaid: $_____**

Prime Contractor Name: Contact Person:

Return one (1) copy of this form to <u>each</u> of the following addresses:

Department of Budget and Management Employee Benefits Division 301 W. Preston Street, 5th Floor Baltimore, MD 21201 ATTN: Napoleon Curameng	MBE Liaison Officer Department of Budget and Management Procurement Unit, Room 109 45 Calvert Street Annapolis, MD 21401

Signature:_____ Date:_____

ATTACHMENT E

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

Whereas Offeror intends to submit a proposal in response to State of Maryland Solicitation No. F10R4200129

(the "RFP"). In order for the Offeror to submit a proposal, it will be necessary for the State to provide the Offeror with access to confidential employee data ("Confidential Data").

Now, Therefore, in consideration of the release of Confidential Information and other promises and covenants contained herein, the parties agree as follows:

1. Offeror will not copy, disclose, publish, release, transfer, disseminate or use for any purpose in any form any of the Confidential Information except in connection with the preparation of its proposal.

2. Each employee or agent of the Offeror who receives or has access to the Confidential Information shall execute a copy of this Agreement and Offeror shall provide the executed Agreement to the State.

3. The original electronic media or computer diskette containing the Confidential Information shall be returned to the State before or coinciding with the submission of Offeror's proposal. No copies of the Confidential Information in any form shall be retained after submission of a proposal. If the Offeror does not submit a proposal, the Offeror shall return the Confidential Information to the Department on or before the due date for proposals.

4. Offeror acknowledges that the disclosure of the Confidential Information may cause irreparable harm to the State and agrees that the State may obtain an injunction to prevent the disclosure or copying of the Confidential Information. The Offeror consents to personal jurisdiction in the Maryland State Courts.

5. Offeror acknowledges that pursuant to Section 11-205.1 of the State Finance and Procurement Article of the Annotated Code of Maryland a person may not willfully make a false or fraudulent statement or representation of a material fact in connection with a procurement contract. Persons making such statements are guilty of a felony and on conviction subject to a fine of not more than $20,000 and/or imprisonment not exceeding 5 years. Offeror further acknowledges that this Agreement is a statement made in connection with a procurement contract.

6. Offeror agrees to indemnify the State of Maryland and to hold it harmless from any and all losses, claims or damages the State may suffer or be exposed to because of any use or disclosure by Offeror of any of the Confidential Information that is not permitted by this Agreement.

7. This Agreement shall be governed by the laws of the State of Maryland.

8. Offeror hereby acknowledges receipt of Confidential Information.

9. The undersigned represents and warrants that he/she has the authority to bind the Offeror to the provisions of this Agreement.

OFFEROR	MARYLAND DEPARTMENT OF BUDGET AND MANAGEMENT
_____	_____
By: Title:	By: Janice Montague Procurement Officer
_____	_____
Date	Date
_____	_____
Witness	Witness

CERTIFICATION OF RETURN OF CONFIDENTIAL DATA

This is to certify that the computer diskette containing confidential employee data is being returned to the State of Maryland and that no copies of such data have been retained except as necessary to prepare this proposal.

OFFEROR

_____

By:
Title:

_____
Date

_____
Witness

RECEIVED BY:

_____
Name:

_____
Date

ATTACHMENT F

Department of Budget and Management
Office of Information Technology

Information Technology
Security Policy and Standards
Version 1

June 2003

Approval Date: June 6, 2003
Approved By: James C. DiPaula
Secretary Department of Budget and Management
Distribution: Executive Branch Chief Information Officers
Initiated By: State Data Security Committee

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Introduction

This document provides policy and supporting standards for information technology security. The policy applies to Executive agencies of the State of Maryland. It establishes general requirements and responsibilities for protecting technology systems, including the responsibility for each agency to have its own technology security plan. The standards establish minimum levels of compliance.

The policy covers such common technologies as computers, data and voice networks, wireless systems, web systems, and many other more specialized resources. The policy is necessitated by the State government's use of information technology to help carry out nearly all of its public services and internal operations. The State's delivery of critical public services depends on availability, reliability and integrity of its information technology systems. Therefore each agency must adopt appropriate methods to protect its technology systems. While some agencies will need to adopt stronger standards and methods, the statewide program based on this policy provides the minimum requirements and a consistent approach for security.

The common security approach also supports compatible security solutions shared among agencies, yielding a better return on technology investment. The security policy and standards will evolve and will require regular updates to remain current.

The policy and standards are issued by the Secretary of Budget and Management under authority granted by the Annotated Code of Maryland, Finance and Procurement Article § 3-401 through 3-413 and § 3-701 through 3-705. It is administered by the Office of Information Technology within the Department of Budget and Management.

Persons with questions or needing further information are encouraged to contact the Information Technology Security Officer in the Office of Information Technology (410-260-7663).

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Information Technology Security Policy

Information and information technology systems are essential assets of the State of Maryland. They are vital to the citizens of the State. Information assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as, to local and federal government entities and to other State agencies. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, and contractors of the State are responsible for protecting information from unauthorized access, modification, disclosure and destruction.

Each agency of the Executive Branch of the State is responsible for compliance with this policy and these standards. The Office of Information Technology (OIT) of the Department of Budget and Management and agency Information Technology (IT) components are to use this policy and these standards as a guide when procuring information technology services, service providers, contractors, software, hardware and network components.

Scope

This policy covers all information that is electronically generated, received, stored, printed, filmed, and typed. In accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705, and with the Executive Order 01.01.1983.18 Privacy and State Data System Security Paragraph 4.D, the provisions of this policy apply to:

All units of the Executive Branch of the State of Maryland for all of their IT systems regardless of who is operating them

All activities and operations required to ensure data security including facility design, physical security, disaster recovery and business continuity planning, use of hardware and operating systems or application software, data disposal, and protection of copyrights and other intellectual property rights

Objectives

This policy and these standards define the minimum requirements to which each State agency, including employees and contractors, must adhere. The primary objectives of the IT Security Policy are:

To establish a secure environment for the processing of data

To reduce information security risk

To communicate the responsibilities for the protection of information

Previous Policy Superseded

This policy and these standards supersede the policies and standards as previously stated in the "State Agency Data Systems Security Practices" as revised (1999).

Authority

The State Data Security Committee and the Office of Information Technology of the Department of Budget and Management have authority to set policy and provide guidance and oversight for security of all IT systems in accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705, and as provided by Executive Order 01.01.1983.18 Privacy and State Data System Security Paragraph 4.D.

Compliance

The head of each agency is responsible for compliance with and enforcement of this Policy.

Agency Chief Information Officers (CIOs) shall develop and implement an Agency IT Security Program to implement this policy and these standards. The Security Program shall include a timetable and controls for compliance. The controls shall include but are not limited to:

- Maintaining the confidentiality, integrity, availability, and accountability of all State information technology applications and services
- Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed
- Ensuring that risks to information security are identified and controls implemented to mitigate these risks
- Implementing processes to ensure that all security services meet the minimum requirements set forth in this policy and the attached standards
- Ensuring that all employees and contractors understand and comply with this Policy, as well as all applicable laws and regulations

Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State's IT assets

Security Program Maintenance and Review

Each State agency will review and update its IT Security Program as needed to conform to changes within the agency or in the State IT Security Program. IT Systems security plans will be reviewed as required by IT security Certification and Accreditation guidelines.

Information Technology Security Deviation and Risk Acceptance

Compliance with this policy shall be planned and achieved as promptly as possible. When an agency determines, in the course of planning or carrying out its IT Security Program, that it is not feasible or practical to comply with a provision or provisions of this policy and attendant standards, or to do so promptly, it shall document the deviation from policy or standards. The documentation, with a timetable for compliance when practicable, shall be prepared as an IT Security Deviation Request.

IT Security Deviation Requests must be filed in accordance with the specifications detailed in the State IT Security Deviation/Risk Acceptance Standard (see section 11, IT Security Deviation/Risk Acceptance Standard). Such deviations require the approval of the agency CIO and the State CIO.

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Key Definitions

Term / Acronym	Definition
Acceptable Risk	A vulnerability that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Accountability	A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual.
Accreditation	The authorization and approval granted to operate a system or network in order to process sensitive data in an operational environment.
Agency	All units of the Executive branch excluding the University System of Maryland.
Authentication	The testing or reconciliation of evidence of a user's identity.
Authorization	The rights and permissions granted to an individual (or process), which enables access to a computer resource.
Authorized Software	Software owned or licensed and used in accordance with the software license or software approved for use by the agency for a specific job function.
Availability	Ensures the reliable and timely access to data or computing resources by the appropriate personnel.
Certification	A technical review made as part of and in support of the accreditation process. Certification shows the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. A judgment and statement of opinion that the accrediting official can use to officially accredit the system is produced.
CIO	Chief Information Officer.
Cold Site	An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed to duplicate the critical systems.
Computer	An electronic, magnetic, optical, or other data processing device or system that performs logical, arithmetic, memory, or storage functions. It includes any data storage facility, or communications facility that is directly related to or operated in conjunction with that device or system.

Term / Acronym	Definition
Confidentiality	Restriction from disclosure, intentionally or unintentionally, to unauthorized persons, processes or devices.
Data Remanence	Residual information left behind once media has been in some way erased.
Incident	Any event, suspected event or attempted action that could pose a threat to the integrity, availability, confidentiality, or accountability of an IT System. Incidents include an attempted security breach, IT System disruption or outage.
Identification	Data uniquely labeling a user to a system.
IDS	Intrusion Detection System
Information Custodian	The business function owner responsible for the information assets for a particular IT System
Integrity	Freedom from corruption or unauthorized modification; internal and external consistency.
IT Systems	Automated systems: communications systems including wireless systems, computer systems, hardware and software, application systems, networks, workstations, servers, personal digital assistants and data on the IT System.
ITEPP	Information Technology Emergency Preparedness Plan, including the business continuity plan, the recovery plan and the business resumption plan.
MCERT	Maryland's Computer Emergency Response Team. Team to be activated in the event of a major IT related disaster.
Network	A system containing any combination of computers, computer terminals, printers, audio or visual display devices or telephones interconnected by telecommunications equipment or cables, used to transmit or receive information.
NIST	National Institute of Standards and Technology.
Non-repudiation	Authentication with a high assurance to be genuine and that can not subsequently be refuted.
OIT	Office of Information Technology within the Department of Budget and Management

Term / Acronym	Definition
Perimeter Access	Access to all entry and exit points of the network, controlled by firewalls and other filtering mechanisms.
Policy	For purposes of this document means both Policy and Standards
PPI	Proprietary and/or Protected Information is information that is not subject to inspection and copying under the Maryland Public Information Act or federal law.
Privacy	The level of confidentiality and protection that a user is given in a system.
PUB	Public Information means information that may be inspected and copied under the Maryland Public Information Act. .
Residual Risk	The portion of risk that remains after security measures have been applied.
Risk	The probability that a particular threat will exploit a particular vulnerability of an IT System.
SDLC	Systems Development Life Cycle as defined in the State of Maryland SDLC Methodology (See www.dbm.state.md.us/html/sdlc.html.)
Software	Computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Responsibility Standard

The following standard sets the minimum level of responsibility for the following individuals and/or groups:

State Data Security Committee
State CIO
Division of Security and Architecture for OIT
Agency
Employees and Contractors

State Data Security Committee

The responsibilities of this committee are outlined in the Executive Order 01.01.1983.18 Privacy and State Data System Security. The committee:

Is the governance body mandated by Executive Order to control data security
Will evaluate the security of State agency systems containing computerized records
Defines IT system security measures to be undertaken
Monitors, through agency self assessment, compliance with the current policy
Reports to the Governor and the Legislative branch the status of data security

State Chief Information Officer

The duties of the State CIO are:

Providing Statewide IT security policy, standards, guidelines, and procedures
Ensuring the State's IT Security Program is established and implemented in compliance with State laws and regulations and federal laws where applicable
Approving deviations to IT security requirements
Reporting to the Governor and the Legislature on the status of the State's IT Security Program
Enforcing State security policy, including establishing the appropriate measures and remedial actions for agencies for non-compliance

Division of Security and Architecture, DBM OIT

The division is responsible for**:**

Developing and maintaining a Statewide Security Program that includes policy, standards, guidelines, procedures, best security practices, IT disaster recovery planning guidelines, IT Security Certification and Accreditation guidelines, security awareness training, and an incident response reporting capability
Identifying security vulnerabilities in State systems and recommending corrective action
Ensuring IT Disaster Recovery plans for critical IT Systems are maintained and that plans are exercised at least annually
Developing and maintaining a Statewide security architecture
Coordinating with State Agencies' CIO, federal and local government, and private industry to resolve security issues and improve security for State systems.
Provide the appropriate guidance to assist agencies in establishing IT Security Programs and compliance with IT Security Policy
Working with other State agencies to establish a coordinated computer incident response effort.

Agency Responsibilities

Each agency is responsible for:

Ensuring the agency's IT Security Program is established and implemented in compliance with State security policies and standards, State and federal laws and regulations as applicable
Implementing a IT Security Certification and Accreditation process for the life cycle of each agency IT System
Reporting to the OIT on the status of the agency's IT Security Program
Enforcing the State IT Security Policy
Managing the program and initiating measures to assure and demonstrate compliance with security requirements

Assuring the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing functions
Assuming the lead role in resolving security and privacy incidents
Documenting and ensuring that a process is implemented for the classification of information in accordance with the Information Sensitivity and Classification Standard
Specifying the level of security required to protect all information assets under their control to comply with this Policy
Generating any IT Information Security Deviation in accordance with the standard
Assuring that an IT disaster recovery plan has been implemented in accordance with the IT Disaster Recovery Plan Guidelines
Development, implementation and testing of the IT Disaster Recovery Plan for critical agency IT Systems
Ensuring a configuration/change management process is used to maintain the security of the IT system
Administering a virus prevention and incident reporting program that coordinates with Maryland's Computer Incident Response Team
Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users

Employees and Contractors

All employees and contract personnel are responsible for:

Being aware of their responsibilities for protecting IT assets of their agency and the State
Exercising due diligence in carrying out the IT Security Policy
Being accountable for their actions relating to their use of all IT Systems
Using IT resources only for intended purposes as defined by policies, laws and regulations of the State

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Information Technology Security Program Standard

Each agency is responsible for developing an IT Security Program for securing the agency's communications systems, computer systems, networks, and data in accordance with the State IT Security Policy. The status of an agency It Security Program will be reported to the State CIO on an annual basis in conjunction with the Annual Data Security Survey. This standard specifies the major components that must be included in every IT Security Program. The following list is not exhaustive; it functions as the minimum set of requirements. At a minimum each program must contain the following elements:

IT Security Policy
Risk Management
Systems Development Life Cycle Methodology
IT Security Certification and Accreditation
IT Disaster Recovery Planning
IT Security Awareness Training
IT Incident Response Process
External Connections Review
IT Security Plan Reporting.

IT Security Policy

Each agency must adopt or develop an agency IT security policy, with standards, and procedures. Policy must meet the minimum requirements as set forth in this Policy.

Risk Management

A risk management process must be implemented to assess the acceptable risk to agency IT Systems as part of a risk-based approach used to determine adequate security for the system. Agencies shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk. Agencies will define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system (see section 5, Nonpublic Information Standard). Refer to NIST Special Publication 800-30 Risk Management Guide for Information Technology at, http://csrc.nist.gov/publications/nistpubs/ for guidance.

Systems Development Life Cycle Methodology

All State systems must include IT security as part of the system development life cycle management process. Refer to the requirements in the State of Maryland SDLC Methodology (See http://www.dbm.maryland.gov/communities/community.asp?UserID=2&CommunityID=226&Folder=2512)

IT Security Certification & Accreditation

Agencies shall develop and implement an IT security certification and accreditation program as part of an overall IT risk management strategy. The program will maintain a catalog of all IT systems and sites (to include existing), ranked by sensitivity and criticality. The cataloged items should be certified and accredited, in order, according to the State IT Security Certification and Accreditation (C&A) Guidelines. All new development shall be conducted using the IT Security C&A process integrated into the development process. (See the State IT Security Certification and Accreditation Guidelines)

IT Disaster Recovery Planning

Agencies shall develop, implement, and test an IT Disaster Recovery plan for each critical IT system to ensure that a contingency system will be available in the event of a disaster to the primary production system. (See the State IT Disaster Recovery Guidelines)

IT Security Awareness, Training, and Education

Agencies shall develop and implement a security awareness, training, and education program for all agency employees and contractors to ensure that all employees and contractors adhere to the State IT Security Policy. (See the State IT Security Awareness Training and Education Training Guidelines)

IT Incident Response Process

Agencies shall be required to participate in the State Incident Response Process by detecting, tracking, logging, and reporting security incidents. (See the Maryland Computer Incident Response Capability Procedures and the Standard Operation Procedures for Electronic Evidence Handling)

External Connections Review

External network connections, non-networked computers and dial-in connections shall be managed, reviewed annually, and documented as prescribed by the Agency IT Security Program. Results will be reported annually as part of the IT security assessment transmitted to the Office of the State CIO and to the SDSC.

IT Security Plan Reporting

Each agency is responsible for reporting on the status of the agency IT Security Program to the State Data Security Committee and the DBM/OIT Division of Security and Architecture on an annual basis. A project plan detailing the projects, estimated costs, and estimated completion time required to bring the agency into compliance with the IT Security Policy must be included in the annual report.

Date Adopted	June 2003
Date of Last Revision	

Nonpublic Information Standard

Agencies shall establish and document a process that protects nonpublic information from disclosure to unauthorized individuals or entities, including other State or federal agencies. The process shall be compliant with the Maryland Public Information Act and any applicable federal laws.

System Sensitivity Designation

Each agency must specify corresponding classification and controls that must be in place for the data within that agency. When the IT System is shared between State units and/or between State, Federal, or local units the highest level of classification will determine the classification of the data or IT System. For example, one agency may categorize the data at a medium level while the second agency may classify the data at a basic level, therefore, the data at both agencies will be at a medium level. All parties sharing the IT System or data must agree to the initial classification and any change in the classification. An IT System shall clearly identify data that is considered PPI and any electronic exchange of data will clearly state that the information is PPI.

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Access Control Standard

All Agencies must ensure that information is accessed by the appropriate persons for authorized use only. To help accomplish this each agency must establish at a minimum the following:

An authentication process to verify the identity of users prior to initiating a session or transaction on an IT system
An authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of "least possible privileges" and " "need-to-know"
An audit trail process to ensure accountability of system and security-related events
A process for ensuring that all systems have the ability to log and report specific security incidents and all attempted violations of system security. In addition, this capability must be enabled at all times
A review process of security audit logs, incident reports and on-line reports at least one (1) time per business day
An investigation process for any unusual or suspicious items, which will incorporate reporting the results as specified in the State IT Incident Response Guideline
An internal assessment process for verifying their compliance to the State IT Security Policy
The processes to establish, manage, and document user id and password administration
A review of access privileges on an annual basis
A process for protecting nonpublic information
A process for explicitly authorizing access to nonpublic information
A process for documenting and escalating all instances of non-compliance with the State IT Security Policy
A segregation of the functions of system administration and security administration to provide separation of duties
Procedures prohibiting security personnel from initiating, programming, processing or authorizing business transactions
Independent audits of agency security administrators security transactions

Authentication

All users must be uniquely identified. Group or shared ids are prohibited unless they are documented as "Functional ids". Functional ids are user accounts associated with a group or role that may be used by multiple individuals (e.g.. Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., RACF id used to run production jobs). Passwords associated with functional ids are exempt from the password restriction on sharing and change requirements specified below.

Password Construction Rules and Change Requirements

Passwords must meet the following usage, construction and change requirements:

The password must not be the same as the user id
Passwords must never be displayed on the screen
The user must select passwords unless randomly generated. Initial passwords and password resets distributed to the user must be issued "pre-expired" forcing the user to change them upon logon
Passwords must be a minimum of eight (8) characters and consist of mixed alphabetic and numeric characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters
Passwords must not contain leading or trailing blanks
Passwords must not contain more than two (2) consecutive identical characters
Password reuse must be prohibited for a minimum of six (6) months.
Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password)
Automated controls must ensure that passwords are changed at least as frequently as every forty-five (45) days
Passwords older than its expiration date must be changed before any other system activity is performed
User ids associated with a password must be disabled after not more than four (4) consecutive failed login attempts and require security administration to reactivate the id
When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established

Authorization

All Agencies must have the following authorization controls implemented:

A documented process to ensure that access privileges are verified at least annually
An automated process to ensure that individual user sessions either time out or initiate a password protected screen saver after a period of thirty (30) minutes of inactivity
A documented process to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hours of the change
A documented process to ensure that physical and logical access is immediately disabled upon a change in employment status where appropriate
An automated process to ensure that user ids are disabled after sixty (60) days of inactivity and deleted after ninety (90) days of inactivity unless they are extended through the explicit approval of the Information Custodian (Note: Functional ids may be exempted from this requirement)
A documented process to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use
A process/system to ensure that access privileges are traceable to a unique user id
An automated display, after a successful logon, showing the date and time of last successful logon and the number of unsuccessful logon attempts since the last successful logon

Audit Trail

The following minimum set of events/actions must be logged and kept as required by State and Federal laws/regulations:

Additions, changes or deletions to data produced by IT systems
Identification and authentication processes
Actions performed by system operators, system managers, system engineers, technical support, and system administrators
Emergency actions performed by support personnel and highly privileged system and security resources

The audit trails must include at least the following information:

Date and time of event
User id of person performing the action
Type of event
Asset or resource name and type of access
Success or failure of event
Source (terminal, port, location, and so forth) where technically feasible

In addition, all lapses in audit trails must be immediately investigated by security administration and the Information Custodian and brought to closure within one (1) week.

Violation Log Management and Review

The Information Custodian must review all violations within one business day of a discovered occurrence. At a minimum the following events should be reviewed:

Two (2) or more failed attempts per system day to access or modify security files, password tables or security devices
Disabled logging or attempts to disable logging
Two (2) or more failed attempts to access or modify nonpublic information within a week
Any unauthorized attempts to modify software or to disable hardware configurations

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Network Security Standard

Agencies must ensure that all information networks are protected from unauthorized access at all entry points. To help accomplish this each agency must, at a minimum:

Establish a process to protect from unauthorized dial-in access
Utilize the State approved banner text (See 7.2)
Establish a process to ensure that all external IP connections are made through a firewall
Implement and monitor an Intrusion Detection Systems (IDS) 24X7X365
Establish a process to ensure that all Service Interface Agreements (SIAs) are managed in accordance with their IT Security Program and the State Policy
Establish a process to ensure that the same level of controls that exist on-site exist for users working remotely
Establish a process to prevent unauthorized mobile code from being loaded onto State IT equipment
Establish a process for ensuring that wireless network connections do not compromise the State's IT Security Program
Establish a process for securing all Private Branch Exchanges (PBXs)

Dial-in Access

The following services are prohibited except where they are specifically approved by the Agency CIO:

Dial-in desktop modems
Use of any type of "remote control" product (e.g., PCAnywhere)
Use of any network-monitoring tool

In addition, the following controls for dial-in users must be implemented:

Unique network access user ids different from their application or network user id.
A minimum prohibition of answer or pickup until after the sixth (6^{th}) ring
Access privileges must be prohibited to any applications except those expressly required (i.e., cannot grant access to entire network, must be application specific)
Annual review of access requirements
Shall not store data unless the data can be protected from unauthorized access, modification, or destruction

Banner Text

The following banner text must be displayed at all system entry points and at all access points to servers, subsystems, etc. where initial user logon occurs:

"**WARNING*****WARNING*****WARNING*****WARNING*****WARNING*****WARNING*
****

This system is available for authorized users only and only within the scope of their authorization. Unauthorized access to and use of this computer are violations of Article 27, Sections 45A and 146 of the Annotated Code of Maryland. All use of the network, including E-mail and the Internet may be monitored. The department has the right to inspect, without notice to the user, any work created on or information transmitted over the network, including all e-mail messages that are sent or received on the network, accessed Internet sites, and information downloaded from or transferred via the Internet. Unauthorized use or misuse of the network may result in disciplinary action.

As with certain other forms of communication, security of e-mail transmissions cannot be absolutely guaranteed. Users should consider whether an alternative form of communication should be used for particularly sensitive information.

****
WARNING***WARNING*****WARNING*****WARNING*****WARNING*****WARNING**

An automatic pause, slow roll rate, or user acknowledgement is required to ensure that the banner can be read. The banner is:

Required for all mainframe, midrange, workstation, personal computer, and network systems
Must be used in addition to, and is not a substitute for, any default banners or copyright/proprietary notices
The first banner that is displayed, except for citizen interfaces where use will negatively impact the citizen. In such cases, this negative impact must be documented by management

Firewalls & Network Devices

State networks will be protected by firewalls at identified points of interface as determined by system sensitivity and data classification. State firewalls should be configured to block all services not required and disable unused ports, hide and prevent direct accessing of State trusted network addresses from untrusted networks, maintain comprehensive audit trails, fail in a closed state and operate on a dedicated platform (device).

All network devices (e.g. servers, routers) shall have all non-needed services disabled and the security for those devices hardened. All devices shall have updates and patches installed on a timely basis to correct significant security flaws. Default or initial passwords shall be changed upon installation of all firewall and network equipment.

Intrusion Detection Systems

State networks will be monitored by an IDS implemented at critical junctures. Host-based, network-based, or a combination of both (preferred) may be utilized. IDS must be monitored 24X7X365. Each agency must establish a severity and escalation list based upon anticipated events that include immediate response capability when appropriate. These plans should be incorporated into the Agency's IT Security Program.

Service Interface Agreement

External network connections shall be permitted only after all approvals required by State law are obtained and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the State agency and the non-State entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system It Security Certification and Accreditation package in the IT System security plan. An SIA shall include:
Purpose and duration of the connection as stated in the agreement, lease, or contract
Points-of-contact and cognizant officials for both the State and non-State organizations
Roles and responsibilities of points-of-contact and cognizant officials for both State and non-State organizations
Security measures to be implemented by the non-State organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection
Requirements for notifying a specified State official within a specified period of time of a security incident on the network, with the recommended time within 4 hours of the incident
A provision allowing the State to periodically test the ability to penetrate the State's network through the external network connection or system

Teleworking

In a telecommuting environment, an agency must require the same level of security on the microcomputer used at home or offsite as the microcomputer used in the workplace.

Mobile Code

Until reliable executable content scanning technology is available to address security concerns with regard to mobile code or executables obtained via the Web, all mobile code or executable content employed within a agency intranet shall be documented in the IT System Security Plan and approved by the Agency CIO.

Wireless Networks

Should agencies establish addressable network segments for the wireless networks, they must ensure that they do not compromise the State IT Security Program. All such networks must at a minimum incorporate the following controls:

Properly configuring of routers
Encrypting the wireless transmissions using 128 bit Virtual Private Networks (VPNs)
Authenticating users with user validation mechanisms more secure than passwords only
Changing the default service set identifier (SSID)
Disabling "broadcast SSID"

Private Branch Exchange (PBX)

If PBX processors require remote vendor maintenance via a dial-in telephone line the following controls must be in place:

A single dedicated telephone line that disables access to the public-switched telephone network
An automated audit trail
Encryption of transmissions
Access controls

Facsimile

Data transmitted by facsimile must be treated in the same manner as any data communicated by network or PBX based on system sensitivity and data classification.

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Physical Security Standard

Physical access to IT information processing, storage areas, and storage devices and its supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas. Agencies must:

Secure IT areas with controls commensurate to the risks
Ensure the secure destruction storage media
Ensure secure media reuse
Ensure secure storage of media
Obtain personnel security clearances where appropriate

Secured IT Areas

Physical access controls must in place for the following:

Data Centers
Areas containing servers and associated media
Networking cabinets and wiring closets
Power and emergency backup equipment
Operations and control areas

Access to data centers and secured areas will be granted for those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be:

Based on frequency of need for access
Approved by the manager responsible for the secured area

Each agency is responsible for:
Issuing picture id badges to all Employees/contractors and ensuring that these badges are openly displayed at all times
Ensuring that all portable storage media such as hard drives, diskettes, magnetic tapes, laptops, and CD are physically secured
Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems
Ensuring that any physical access controls are auditable

Storage Media Disposal

When no longer usable diskettes, compact disks, tape cartridges, ribbons, and other similar items shall be destroyed by a NIST approved method such as shredding, incineration, overwriting, or degaussing. All IT equipment shall not be released from an agency's control until the equipment is sanitized and all stored information has been cleared. This requirement applies to all permanent disposal of equipment regardless of the identity of the recipient. This includes equipment transferred to schools, as well as equipment maintenance and repair.

Media Reuse

When no longer required for mission or project completion, media (tapes, disks, hard drives, etc.) to be used by another person within the agency shall be overwritten with software and protected consistent with the data sensitivity at which IT storage media were previously used. The procedures shall be documented in the IT System Security Plan.

Storage And Marking

IT Systems and electronic media shall be protected and marked in accordance with the data sensitivity. Users shall not store data on electronic media that cannot be adequately secured against unauthorized access.

Personnel

Security clearances are required for personnel as determined by the system sensitivity and data classification designation. Agencies will ensure that an appropriate background investigation (e.g., CJIS, State Police) has been completed on personnel as necessary. Agencies will maintain personnel clearance information on file.

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Microcomputer/PC/Laptop Security Standard

Agencies must ensure that all microcomputer (i.e., workstation, desktop computers, laptops computers, PDA's, and any other portable device that processes data) are secured against unauthorized access. The level of controls should be commensurate with the information accessed, stored, or processed on these devices. To help accomplish this each agency must establish at a minimum the following:

General controls
Virus protection
Software licensing and use controls
Laptop security and mobile computing controls
Protection from personally owned microcomputers

General Controls

All microcomputers that store and/or access nonpublic information must implement the following controls:

User id and password to control access at logon
Encryption to protect directories, sub-directories, and/or files containing nonpublic information
Virus Protection

Standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers. These programs must:

- Be configured to run checks for viruses at startup and operate in memory-resident mode to check for viruses during normal processing
- Be updated as soon as updates are available from the vendor
- Be configured to prevent connection to the network unless the accessing microcomputer has the latest version of the virus product and update installed

Software Licenses And Use

Agencies shall establish procedures to ensure compliance with State Copyright Policy, Department of Budget and Management Policy Number 95-1, and assure that software installed on agency IT Systems is incorporated into the SDLC management process.

Unless specifically approved by the Agency CIO and the agency head, personal or corporate IT equipment shall not have State licensed software installed and shall not be used to process or transmit PPI. Only State owned and authorized computer software is to be used on standalone or networked computer equipment.

Authorized software packages are those approved by the Agency CIO. Executable modules cannot be downloaded from the Internet unless authorized by the Agency CIO and agency network administrator. Agencies should designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

Laptop Security And Mobile Computing

Laptops and mobile computing devices are not authorized to process or store nonpublic information unless approved in writing by the agency network support administrator, the Agency CIO and the agency head. Laptops and mobile computing devices which include personal digital assistants approved for processing PPI information cannot be connected to State networks or systems unless the network or system is certified and accredited for that function. In such cases the IT Security Program will identify the devices that can be used to access the network or the system, the purposes for the access, and the security controls for the connection.

Personally Owned Data Processing Equipment

Processing or storing PPI on personal or contractor owned data processing equipment is prohibited unless approved by the agency network support administrator, the Agency CIO and the agency head.

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Encryption Standard

Agencies must ensure that encryption is utilized to protect any non-public information when it is stored or transmitted through any environment. IT Systems employing encryption must comply with all applicable Federal Information Processing Standards (FIPS) publications and guidelines for encryption (References located at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf),

To help accomplish this each agency using encryption must establish at a minimum the following:

Secure cryptographic keys
Use of Public Key Cryptography methods approved by the State CIO
All cryptographic keys must have a designated, unique owner.

Key change intervals shall be established by each agency, but must be no longer than the following:

Master keys must be changed once per year, if the product allows
Key encrypting keys (e.g., asymmetric encrypting a symmetric) must be changed at a minimum of every six (6) months
Link encrypting keys must be changed every thirty (30) days

Keys must be distributed in a secure manner ensuring that the entire key is not exposed while in transit to any one individual at any one time.

Default cryptographic keys may not be utilized, except they may be utilized for emergency recovery, system calibration or vendor certification purposes. In such cases, a documented process describing the storage, maintenance, use and destruction of these keys must be in place.

Public Key Technology (Asymmetric)

All public key management systems, Certification Authorities (CAs), key distribution systems, key recovery systems, and cross-certification processes must be approved by the State CIO and the State Data Security Committee. Every public key and certificate must have an associated scope of use, which must be checked by any user or server that accepts or relies upon the certificate.

The process for issuing digital certificates must:

Establish the identity of the subject
Establish that the subject is the holder of the associated private keys

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

IT Information Security Deviation/Risk Acceptance Standard

An Information Security Deviation Request/Risk Acceptance form must be completed by the agency if it determines that it cannot or will not comply with the State IT Security Policy. All deviation requests require the approval of the agency CIO, Information Custodian, agency head, and the State CIO.

General Requirements

Proposed deviations will be considered on an individual basis

Where appropriate, a risk assessment will be performed to evaluate the threats, countermeasures and extenuating circumstances associated with the proposed deviation and its impact on IT systems

Requests for deviations must by completed by the requesting Information Custodian and must be made in writing

Deviations will be granted for a maximum period of twelve (12) months after which time the deviation will be considered expired and require renewal by the Information Custodian

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

Use of Electronic Communications Standard

This standard applies to information technology security, however, it is not inclusive of other State policies and regulations that may further apply to the use of electronic communications.

The use of the Internet, E-mail and other State computing equipment, networks and communication facilities is provided to State employees and contract employees as electronic tools to perform their job functions. Information communicated electronically through email, the Internet or sharing of electronic documents is subject to State laws, regulations, policies and other requirements, as is information communicated in other written forms and formats. Access to State agency email or Internet services may be wholly or partially restricted without prior notice and without user consent.

12.1 Internet and Electronic Communications

Users accessing the Internet or other State electronic communications through State resources may be monitored. Agencies shall develop standards consistent with all State policies and standards regarding E-mail, Internet use, and use of other computer resources. Electronic communications that are not secure or encrypted should not be used to send information that is nonpublic information.

12.2 Computer Software

Users, unless specifically authorized because of their job functions, are not permitted use unauthorized software (e.g., downloaded software, pirated software, software not licensed to the State, software brought from home). This includes, but is not limited to programs, executable modules and screen savers. (*Refer to additional guidance in the State of Maryland Software Code of Ethics Form, Department of Budget and Management's Policy Number 95-1)*

12.3 IT Incident and Advisories

Each agency shall notify its staff of the personnel designated to provide authenticated notices of IT incidents and advisories. Employees other than the designated personnel shall not forward IT Incident advisories to agency staff. If an advisory comes to an employee, the employee shall forward it to the designated personnel for evaluation.

Date Adopted	June 2003
Date of Last Revision	

Standards Self-Assessment Checklist

The purpose of this checklist is to assist individuals designing new application, architectures, or modifying existing systems. The checklist is designed to provide questions pertaining to the majority of the IT Security Standards. It does not include many of the administrative functions detailed in the IT Security Standards and it should not be considered a substitute for reading the IT Security Policy. The checklist had been designed so that an answer of "NO" indicates a potential security issue that requires further investigation.

IT Security Program Standard	N/A	Yes	No
1. Does the agency have an IT Security Program? *(Section 4)*			
2. Has the agency adopted the State IT Security Policy or developed its own policy? *(Section 4.1)*			
3. Has the agency adopted the State IT Security Standards or developed its own standards? *(Section 4.1*			
4. Has the agency implemented a risk management process for determining adequate security levels for the IT systems? *(Section 4.2)*			
5. Is IT security included as part of the SDLC? *(Section 4.3)*			
6. Has the agency developed and implemented an IT security certification and accreditation program as part of its overall IT risk management strategy? *(Section 4.4)*			
7. Has the agency developed, implemented, and tested and IT Disaster Recovery plan for each critical IT system? *(Section 4.5)*			
8. Has the agency developed and implemented a security awareness, training, and education program for all agency employees and contractors? *(Section 4.6)*			
9. Is the agency participating in the State Incident Response Process? *(Section 4.7)*			
10. Are all external network connections, non-networked computers and dial-in connections documented and reviewed for security implications on an annual basis? *(Section 4.8)*			
11. Is the agency reporting the status of its IT Security Program to the State Data Security Committee and the DBM/OIT Division of Security and Architecture on an annual basis? *(Section 4.9)*			
Nonpublic Information Standard			
12. Has the agency established and documented a process that protects nonpublic information from disclosure to unauthorized individuals or entities? *(Section 5)*			
13. Has the agency documented a process for protection for nonpublic information? *(Section 5)*			
14. Has the agency specified the corresponding controls that must be in place for each level of classification? *(Section 5.1)*			
Access Control Standard			
15. Is the agency ensuring that information is accessed only by the appropriate persons for authorized use? *(Section 6)*			
16. Has an authentication process verifying the identity of users prior to initiating a session or transaction been implemented for all systems containing nonpublic information? *(Section 6)*			
17. Has an authorization process that specifically grants access to nonpublic information that ensures that the access is strictly controlled, audited, and supports the concepts of "least possible privileges" and "need-to-know" been implemented? *(Section 6)*			
18. Has an audit process been implemented to ensure that accountability of system and security-related events? *(Section 6)*			
19. Has a process been implemented to ensure that all systems have the ability to log and report specific security incidents and attempted violations? *(Section 6)*			
20. Is there a segregation of the functions of system administration and security			

administration providing separation of duties? *(Section 6)*			
21. Is there an independent verification of security transactions? *(Section 6)*			
22. Are group or shared ids prohibited? *(Section 6.1)*			
23. Are passwords prohibited from being the same as the user id? *(Section 6.1)*			
24. Are passwords prohibited from being displayed in clear-text on the screen? *(Section 6.1)*			
25. Are initial passwords and password resets distributed to the user in a "pre-expired" state? *(Section 6.1)*			
26. Are passwords selected by the user or randomly generated? *(Section 6.1)*			
27. Are passwords required to be a minimum of eight (8) characters? *(Section 6.1)*			
28. Are passwords required to be a mix of alphabetic and numeric characters? *(Section 6.1)*			
29. Are passwords prohibited from containing leading or trailing blanks? *(Section 6.1)*			
30. Are passwords prohibited from containing more than two (2) consecutive identical characters? *(Section 6.1)*			
31. Are passwords prohibited from being reused for a minimum of six (6) months? *(Section 6.1)*			
32. Have automated controls been implemented to ensure that passwords are changed at least as frequently as every forty-five (45) days? *(Section 6.1)*			
33. Are user ids disabled after not more than four (4) consecutive failed login attempts? *(Section 6.1)*			
34. Do disabled ids require security administration to reactivate the id? *(Section 6.1)*			
35. Has a documented process been implemented to ensure that access privileges are verified at least annually? *(Section 6.2)*			
36. Has an automated process been implemented to ensure that individual user sessions either time out or initiate a password protected screen saver every thirty (30) minutes? *(Section 6.2)*			
37. Has a documented process been implemented to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hour of the change? *(Section 6.2)*			
38. Has a documented process been implemented to ensure that physical and logical access is immediately disabled upon a change in status where appropriate? *(Section 6.2)*			
39. Has an automated process been implemented to ensure that user ids are disabled after sixty (60) days of inactivity? *(Section 6.2)*			
40. Has an automated process been implemented to ensure that user ids are deleted after ninety (90) days of inactivity? *(Section 6.2)*			
41. Has a documented process been implemented to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use? *(Section 6.2)*			
42. Has an automated process been implemented to ensure that access privileges are traceable to a unique id? *(Section 6.2)*			
43. Has an automated display been implemented showing the date and time of the last successful logon and number of failed logon attempts? *(Section 6.2)*			
44. Are audit trails maintained as required by Federal or State laws/regulations? *(Section 6.3)*			
45. Do the audit trails capture all additions, changes, or data produced by IT Systems? *(Section 6.3)*			
46. Do the audit trails capture all identification and authentication processes? *(Section 6.3)*			
47. Do the audit trails capture all actions performed by the system operators, system managers, system engineers (technical support), and system administrators? *(Section 6.3)*			
48. Do the audit trails capture all the emergency actions performed by support personnel and highly privileged system and security resources? *(Section 6.3)*			
49. Do the audit trails contain the date and time of the event? *(Section 6.3)*			

50. Do the audit trails contain the user id of the person performing the action? *(Section 6.3)*			
51. Do the audit trails contain the type of event (e.g., read, update, delete, etc.)? *(Section 6.3)*			
52. Do the audit trails contain the resource name? *(Section 6.3)*			
53. Do the audit trails contain the success or failure of the event? *(Section 6.3)*			
54. Do the audit trails show source (e.g., terminal, port, etc.) where technically feasible? *(Section 6.3)*			
55. Are all lapses in audit trails immediately investigated by the Information Custodian and brought to closure within one (1) week? *(Section 6.3)*			
56. Are the violation logs reviewed by the Information Custodian within one (1) business day? *(Section 6.4)*			
Network Security Standard			
57. Has a process been established to protect from unauthorized dial-in access? *(Section 7)*			
58. Is the State approved banner text being presented at all initial login points? *(Section 7)*			
59. Has a process been implemented to ensure that all external IP connections are protected by a firewall? *(Section 7)*			
60. Is IDS implemented and monitored 24X7X365? *(Section 7)*			
61. Has a process been implemented to ensure that all SIAs are managed in accordance with the IT Security Program, Policy, and Standards? *(Section 7 and 7.5)*			
62. Have controls been imp lemented to ensure that remote users have the same level of controls that exist onsite? *(Section 7 and 7.6)*			
63. Have controls been implemented to prevent unauthorized mobile code from being loaded onto State IT equipment? *(Section 7 and 7.7)*			
64. Has a process been implemented to ensure that any wireless connections do not compromise the State's Security Program? *(Section 7 and 7.8)*			
65. Have all PBXs been secured? *(Section 7 and 7.9)*			
66. Have dial-in modems been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
67. Have all types of "remote control" (e.g., PCAnywhere) been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
68. Have all network-monitoring tools been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
69. Are dial-in users required to use an id that is different from their application or network user id? *(Section 7.1)*			
70. Is the call pickup for modems set to a minimum of six (6) rings? *(Section 7.1)*			
71. Are dial-in users restricted to accessing only specific applications or servers (i.e., do not have access to the entire network)? *(Section 7.1)*			
72. Is an annual review performed for all dial-in users? *(Section 7.1)*			
73. Are all firewalls configured to block unnecessary services? *(Section 7.3)*			
74. Are security updates and patches applied to all network devices in a timely manner? *(Section 7.3)*			
75. Has the agency documented and implemented a severity and escalation list based upon anticipated events that includes immediate response capability when appropriate? *(Section 7.4)*			
Physical Security Standard			
76. Have all IT areas been secured with controls commensurate to the risks? *(Section 8, 8.1, and 8.5)*			
77. Has a process been implemented to ensure the secure storage, reuse, and/or destruction of storage media? *(Section 8, 8.2, 8.3, and 8.4)*			
Microcomputer/PC/Laptop Security Standard			
78. Have all microcomputers (i.e., workstations, desktop computers, laptop computers, PDAs, and other portable devices) been secured against unauthorized access?			

(Section 9)			
79. Do all microcomputers that store, process, and/or access non-public information require a unique user id and password for access? *(Section 9.1)*			
80. Is virus protection installed on all microcomputers? *(Section 9.1)*			
81. Are the virus definitions updated weekly? *(Section 9.1)*			
82. Are virus definitions updated immediately when circumstances warrant such action (e.g., to control the spread of a new virulent strain)? *(Section 9.1)*			
83. Are microcomputer and/or the servers configured to run checks for viruses at startup and to operate in memory resident mode to check for viruses during normal processing? *(Section 9.1)*			
84. Are the networks configured to prevent connection to microcomputers unless the latest version of the virus product update has been installed and running? *(Section 9.1)*			
85. Has the agency established procedures to ensure compliance with software licensing and use? *(Section 9.2)*			
86. Are laptops and mobile computing devices prohibited from accessing or storing nonpublic information unless approved in writing by the Information Custodian? *(Section 9.4)*			
87. Is personally owned data processing equipment (i.e., not owned by the State) prohibited from accessing systems with nonpublic information? *(Section 9.5)*			
Encryption Standard			
88. Is encryption utilized to protect all information classified as NON-PUBLIC INFORMATION-High when it is stored or transmitted? *(Section 10)*			
89. Do all IT Systems employing encryption comply with applicable Federal Information Processing Standards? *(Section 10)*			
90. Are all cryptographic keys secure from unauthorized access? *(Section 10)*			
91. Have all Public Key Cryptography methods been approved by the State CIO and the Data Security Committee? *(Section 10 and 10.2)*			
92. Do all cryptographic keys have a designated, unique owner? *(Section 10.1)*			
93. Are master keys changed at least annually? *(Section 10.1)*			
94. Are key encrypting keys (e.g., asymmetric encrypting a symmetric) changed at least every six (6) months? *(Section 10.1)*			
95. Are link encrypting keys changed at least every thirty (30) days? *(Section 10.1)*			
96. Are keys distributed in a secure manner? *(Section 10.1)*			
97. Are default cryptographic keys prohibited except for emergency recovery? *(Section 10.1)*			
98. Has an associated scope of use be documented for every public key and certificate? *(Section 10.2)*			
99. Has a secure process been implemented for issuing digital certificates? *(Section 10.2)*			
IT Information Security Deviation/Risk Acceptance Standard			
100. Has an IT Information Security Deviation been completed for all instances on non-compliance with the State IT Security Policy? *(Section 11)*			
101. Has the Information Custodian renewed applicable IT Information Security Deviations that are still enforce after 12 months? *(Section 11)*			
Use of Electronic Communications Standard			
102. Has the agency ensured that all employees/contractors understand that the use of the Internet, E-mail and other State computing equipment, networks and communication facilities are provided to meet their job functions and as such all information is State property and is not subject to privacy? *(Section 12)*			

13 Standards Self-Assessment Checklist

The purpose of this checklist is to assist individuals designing new application, architectures, or modifying existing systems. The checklist is designed to provide questions pertaining to the majority of the IT Security Standards. It does not include many of the administrative functions detailed in the IT Security Standards and it should not be considered a

substitute for reading the IT Security Policy. The checklist had been designed so that an answer of "NO" indicates a potential security issue that requires further investigation.

IT Security Program Standard	N/A	Yes	No
103. Does the agency have an IT Security Program? *(Section 4)*			
104. Has the agency adopted the State IT Security Policy or developed its own policy? *(Section 4.1)*			
105. Has the agency adopted the State IT Security Standards or developed its own standards? *(Section 4.1*			
106. Has the agency implemented a risk management process for determining adequate security levels for the IT systems? *(Section 4.2)*			
107. Is IT security included as part of the SDLC? *(Section 4.3)*			
108. Has the agency developed and implemented an IT security certification and accreditation program as part of its overall IT risk management strategy? *(Section 4.4)*			
109. Has the agency developed, implemented, and tested and IT Disaster Recovery plan for each critical IT system? *(Section 4.5)*			
110. Has the agency developed and implemented a security awareness, training, and education program for all agency employees and contractors? *(Section 4.6)*			
111. Is the agency participating in the State Incident Response Process? *(Section 4.7)*			
112. Are all external network connections, non-networked computers and dial-in connections documented and reviewed for security implications on an annual basis? *(Section 4.8)*			
113. Is the agency reporting the status of its IT Security Program to the State Data Security Committee and the DBM/OIT Division of Security and Architecture on an annual basis? *(Section 4.9)*			
Nonpublic Information Standard			
114. Has the agency established and documented a process that protects nonpublic information from disclosure to unauthorized individuals or entities? *(Section 5)*			
115. Has the agency documented a process for protection for nonpublic information? *(Section 5)*			
116.	**N/A**	**Yes**	**No**
117. Has the agency specified the corresponding controls that must be in place for each level of classification? *(Section 5.1)*			
Access Control Standard			
118. Is the agency ensuring that information is accessed only by the appropriate persons for authorized use? *(Section 6)*			
119. Has an authentication process verifying the identity of users prior to initiating a session or transaction been implemented for all systems containing nonpublic information? *(Section 6)*			
120. Has an authorization process that specifically grants access to nonpublic information that ensures that the access is strictly controlled, audited, and supports the concepts of "least possible privileges" and "need-to-know" been implemented? *(Section 6)*			
121. Has an audit process been implemented to ensure that accountability of system and security-related events? *(Section 6)*			
122. Has a process been implemented to ensure that all systems have the ability to log and report specific security incidents and attempted violations? *(Section 6)*			
123. Is there a segregation of the functions of system administration and security administration providing separation of duties? *(Section 6)*			
124. Is there an independent verification of security transactions? *(Section 6)*			
125. Are group or shared ids prohibited? *(Section 6.1)*			
126. Are passwords prohibited from being the same as the user id? *(Section 6.1)*			
127. Are passwords prohibited from being displayed in clear-text on the screen? *(Section 6.1)*			
128. Are initial passwords and password resets distributed to the user in a "pre-expired"			

state? *(Section 6.1)*			
129. Are passwords selected by the user or randomly generated? *(Section 6.1)*			
130. Are passwords required to be a minimum of eight (8) characters? *(Section 6.1)*			
131. Are passwords required to be a mix of alphabetic and numeric characters? *(Section 6.1)*			
132. Are passwords prohibited from containing leading or trailing blanks? *(Section 6.1)*			
133. Are passwords prohibited from containing more than two (2) consecutive identical characters? *(Section 6.1)*			
134. Are passwords prohibited from being reused for a minimum of six (6) months? *(Section 6.1)*			
135. Have automated controls been implemented to ensure that passwords are changed at least as frequently as every forty-five (45) days? *(Section 6.1)*			
136. Are user ids disabled after not more than four (4) consecutive failed login attempts? *(Section 6.1)*			
137. Do disabled ids require security administration to reactivate the id? *(Section 6.1)*			
138. Has a documented process been implemented to ensure that access privileges are verified at least annually? *(Section 6.2)*			
139. Has an automated process been implemented to ensure that individual user sessions either time out or initiate a password protected screen saver every thirty (30) minutes? *(Section 6.2)*			
140. Has a documented process been implemented to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hour of the change? *(Section 6.2)*			
141. Has a documented process been implemented to ensure that physical and logical access is immediately disabled upon a change in status where appropriate? *(Section 6.2)*			
142. Has an automated process been implemented to ensure that user ids are disabled after sixty (60) days of inactivity? *(Section 6.2)*			
143. Has an automated process been implemented to ensure that user ids are deleted after ninety (90) days of inactivity? *(Section 6.2)*			
144. Has a documented process been implemented to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use? *(Section 6.2)*			
145. Has an automated process been implemented to ensure that access privileges are traceable to a unique id? *(Section 6.2)*			
146. Has an automated display been implemented showing the date and time of the last successful logon and number of failed logon attempts? *(Section 6.2)*			
147. Are audit trails maintained as required by Federal or State laws/regulations? *(Section 6.3)*			
148. Do the audit trails capture all additions, changes, or data produced by IT Systems? *(Section 6.3)*			
149. Do the audit trails capture all identification and authentication processes? *(Section 6.3)*			
150. Do the audit trails capture all actions performed by the system operators, system managers, system engineers (technical support), and system administrators? *(Section 6.3)*			
151. Do the audit trails capture all the emergency actions performed by support personnel and highly privileged system and security resources? *(Section 6.3)*			
152. Do the audit trails contain the date and time of the event? *(Section 6.3)*			
153. Do the audit trails contain the user id of the person performing the action? *(Section 6.3)*			
154. Do the audit trails contain the type of event (e.g., read, update, delete, etc.)? *(Section 6.3)*			
155. Do the audit trails contain the resource name? *(Section 6.3)*			
156. Do the audit trails contain the success or failure of the event? *(Section 6.3)*			
157. Do the audit trails show source (e.g., terminal, port, etc.) where technically			

feasible? *(Section 6.3)*			
158. Are all lapses in audit trails immediately investigated by the Information Custodian and brought to closure within one (1) week? *(Section 6.3)*			
159. Are the violation logs reviewed by the Information Custodian within one (1) business day? *(Section 6.4)*			
Network Security Standard			
160. Has a process been established to protect from unauthorized dial-in access? *(Section 7)*			
161. Is the State approved banner text being presented at all initial login points? *(Section 7)*			
162. Has a process been implemented to ensure that all external IP connections are protected by a firewall? *(Section 7)*			
163. Is IDS implemented and monitored 24X7X365? *(Section 7)*			
164. Has a process been implemented to ensure that all SIAs are managed in accordance with the IT Security Program, Policy, and Standards? *(Section 7 and 7.5)*			
165. Have controls been implemented to ensure that remote users have the same level of controls that exist onsite? *(Section 7 and 7.6)*			
166. Have controls been implemented to prevent unauthorized mobile code from being loaded onto State IT equipment? *(Section 7 and 7.7)*			
167. Has a process been implemented to ensure that any wireless connections do not compromise the State's Security Program? *(Section 7 and 7.8)*			
168. Have all PBXs been secured? *(Section 7 and 7.9)*			
169. Have dial-in modems been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
170. Have all types of "remote control" (e.g., PCAnywhere) been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
171. Have all network-monitoring tools been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
172. Are dial-in users required to use an id that is different from their application or network user id? *(Section 7.1)*			
173. Is the call pickup for modems set to a minimum of six (6) rings? *(Section 7.1)*			
174. Are dial-in users restricted to accessing only specific applications or servers (i.e., do not have access to the entire network)? *(Section 7.1)*			
175. Is an annual review performed for all dial-in users? *(Section 7.1)*			
176. Are all firewalls configured to block unnecessary services? *(Section 7.3)*			
177. Are security updates and patches applied to all network devices in a timely manner? *(Section 7.3)*			
178. Has the agency documented and implemented a severity and escalation list based upon anticipated events that includes immediate response capability when appropriate? *(Section 7.4)*			
Physical Security Standard			
179. Have all IT areas been secured with controls commensurate to the risks? *(Section 8, 8.1, and 8.5)*			
180. Has a process been implemented to ensure the secure storage, reuse, and/or destruction of storage media? *(Section 8, 8.2, 8.3, and 8.4)*			
Microcomputer/PC/Laptop Security Standard			
181. Have all microcomputers (i.e., workstations, desktop computers, laptop computers, PDAs, and other portable devices) been secured against unauthorized access? *(Section 9)*			
182. Do all microcomputers that store, process, and/or access non-public information require a unique user id and password for access? *(Section 9.1)*			
183. Is virus protection installed on all microcomputers? *(Section 9.1)*			
184. Are the virus definitions updated weekly? *(Section 9.1)*			
185. Are virus definitions updated immediately when circumstances warrant such action (e.g., to control the spread of a new virulent strain)? *(Section 9.1)*			

186. Are microcomputer and/or the servers configured to run checks for viruses at startup and to operate in memory resident mode to check for viruses during normal processing? *(Section 9.1)*			
187. Are the networks configured to prevent connection to microcomputers unless the latest version of the virus product update has been installed and running? *(Section 9.1)*			
188. Has the agency established procedures to ensure compliance with software licensing and use? *(Section 9.2)*			
189. Are laptops and mobile computing devices prohibited from accessing or storing nonpublic information unless approved in writing by the Information Custodian? *(Section 9.4)*			
190. Is personally owned data processing equipment (i.e., not owned by the State) prohibited from accessing systems with nonpublic information? *(Section 9.5)*			
Encryption Standard			
191. Is encryption utilized to protect all information classified as NON-PUBLIC INFORMATION-High when it is stored or transmitted? *(Section 10)*			
192. Do all IT Systems employing encryption comply with applicable Federal Information Processing Standards? *(Section 10)*			
193. Are all cryptographic keys secure from unauthorized access? *(Section 10)*			
194. Have all Public Key Cryptography methods been approved by the State CIO and the Data Security Committee? *(Section 10 and 10.2)*			
195. Do all cryptographic keys have a designated, unique owner? *(Section 10.1)*			
196. Are master keys changed at least annually? *(Section 10.1)*			
197. Are key encrypting keys (e.g., asymmetric encrypting a symmetric) changed at least every six (6) months? *(Section 10.1)*			
198. Are link encrypting keys changed at least every thirty (30) days? *(Section 10.1)*			
199. Are keys distributed in a secure manner? *(Section 10.1)*			
200. Are default cryptographic keys prohibited except for emergency recovery? *(Section 10.1)*			
201. Has an associated scope of use be documented for every public key and certificate? *(Section 10.2)*			
202. Has a secure process been implemented for issuing digital certificates? *(Section 10.2)*			
IT Information Security Deviation/Risk Acceptance Standard			
203. Has an IT Information Security Deviation been completed for all instances on non-compliance with the State IT Security Policy? *(Section 11)*			
204. Has the Information Custodian renewed applicable IT Information Security Deviations that are still enforce after 12 months? *(Section 11)*			
Use of Electronic Communications Standard			
205. Has the agency ensured that all employees/contractors understand that the use of the Internet, E-mail and other State computing equipment, networks and communication facilities are provided to meet their job functions and as such all information is State property and is not subject to privacy? *(Section 12)*			

ATTACHMENT G

NAIC 120-1 MODEL COB
CONTRACT PROVISIONS

MODEL COB CONTRACT PROVISIONS

COORDINATION OF THIS GROUP CONTRACT'S BENEFITS WITH OTHER BENEFITS

This coordination of benefits (COB) provision applies when a person has health care coverage under more than one plan. "Plan" is defined below.

The order of benefit determination rules below determine which plan will pay as the primary plan. The primary plan that pays first pays without regard to the possibility that another plan may cover some expenses. A secondary plan pays after the primary plan and may reduce the benefits it pays so that payments from all group plans do not exceed 100% of the total allowable expense.

DEFINITIONS

A. A "plan" is any of the following that provides benefits or services for medical or dental care or treatment. However, if separate contracts are used to provide coordinated coverage for members of a group, the separate contracts are considered parts of the same plan and there is no COB among those separate contracts.

(1) "Plan" includes: group insurance, closed panel or other forms of group or group-type coverage (whether insured or uninsured); hospital indemnity benefits in excess of $200 per day; medical care components of group long-term care contracts, such as skilled nursing care; medical benefits under group or individual automobile contracts; and Medicare or other governmental benefits, as permitted by law.

(2) "Plan" does not include: individual or family insurance; closed panel or other individual coverage (except for group-type coverage); amounts of hospital indemnity insurance of $200 or less per day; school accident type coverage, benefits for non-medical components of group long-term care policies; Medicare supplement policies, Medicaid policies and coverage under other governmental plans, unless permitted by law.

Each contract for coverage under (1) or (2) is a separate plan. If a plan has two parts and COB rules apply only to one of the two, each of the parts is treated as a separate plan.

B. The order of benefit determination rules determine whether this plan is a "primary plan" or "secondary plan" when compared to another plan covering the person.

When this plan is primary, its benefits are determined before those of any other plan and without considering any other plan's benefits. When this plan is secondary, its benefits are determined after those of another plan and may be reduced because of the primary plan's benefits.

C. "Allowable expense" means a health care service or expense, including deductibles and copayments, that is covered at least in part by any of the plans covering the person. When a plan provides benefits in the form of services, (for example an HMO) the reasonable cash value of each service will be considered an allowable expense and a benefit paid. An expense or service that is not covered by any of the plans is not an allowable expense. The following are examples of expenses or services that are not allowable expenses:

(1) If a covered person is confined in a private hospital room, the difference between the cost of a semi-private room in the hospital and the private room, (unless the patient's stay in a private hospital room is medically necessary in terms of generally accepted medical practice, or one of the plans routinely provides coverage for hospital private rooms) is not an allowable expense.

(2) If a person is covered by 2 or more plans that compute their benefit payments on the basis of usual and customary fees, any amount in excess of the highest of the usual and customary fees for a specific benefit is not an allowable

expense.

(3) If a person is covered by 2 or more plans that provide benefits or services on the basis of negotiated fees, an amount in excess of the highest of the negotiated fees is not an allowable expense.

(4) If a person is covered by one plan that calculates its benefits or services on the basis of usual and customary fees and another plan that provides its benefits or services on the basis of negotiated fees, the primary plan's payment arrangements shall be the allowable expense for all plans.

(5) The amount a benefit is reduced by the primary plan because a covered person does not comply with the plan provisions. Examples of these provisions are second surgical opinions, precertification of admissions, and preferred provider arrangements.

D. "Claim determination period" means a calendar year. However, it does not include any part of a year during which a person has no coverage under this plan, or before the date this COB provision or a similar provision takes effect.

E. "Closed panel plan" is a plan that provides health benefits to covered persons primarily in the form of services through a panel of providers that have contracted with or are employed by the plan, and that limits or excludes benefits for services provided by other providers, except in cases of emergency or referral by a panel member.

F. "Custodial parent" means a parent awarded custody by a court decree. In the absence of a court decree, it is the parent with whom the child resides more than one half of the calendar year without regard to any temporary visitation.

ORDER OF BENEFIT DETERMINATION RULES

When two or more plans pay benefits, the rules for determining the order of payment are as follows:

A. The primary plan pays or provides its benefits as if the secondary plan or plans did not exist.

B. A plan that does not contain a coordination of benefits provision that is consistent with this regulation is always primary. There is one exception: coverage that is obtained by virtue of membership in a group that is designed to supplement a part of a basic package of benefits may provide that the supplementary coverage shall be excess to any other parts of the plan provided by the contract holder. Examples of these types of situations are major medical coverages that are superimposed over base plan hospital and surgical benefits, and insurance type coverages that are written in connection with a closed panel plan to provide out-of-network benefits.

C. A plan may consider the benefits paid or provided by another plan in determining its benefits only when it is secondary to that other plan.

D. The first of the following rules that describes which plan pays its benefits before another plan is the rule to use.

(1) Non-Dependent or Dependent. The plan that covers the person other than as a dependent, for example as an employee, member, subscriber or retiree is primary and the plan that covers the person as a dependent is secondary. However, if the person is a Medicare beneficiary and, as a result of federal law, Medicare is secondary to the plan covering the person as a dependent; and primary to the plan covering the person as other than a dependent (e.g. a retired employee); then the order of benefits between the two plans is reversed so that the plan covering the person as an employee, member, subscriber or retiree is secondary and the other plan is primary.

(2) Child Covered Under More Than One Plan. The order of benefits when a child is covered by more than one plan is:

(a) The primary plan is the plan of the parent whose birthday is earlier in the year if:

. The parents are married;

. The parents are not separated (whether or not they ever have been married); or

. A court decree awards joint custody without specifying that one party has the responsibility to provide health care coverage.

If both parents have the same birthday, the plan that covered either of the parents longer is primary.

(b) If the specific terms of a court decree state that one of the parents is responsible for the child's health care expenses or health care coverage and the plan of that parent has actual knowledge of those terms, that plan is primary. This rule applies to claim determination periods or plan years commencing after the plan is given notice of the court decree.

(c) If the parents are not married, or are separated (whether or not they ever have been married) or are

divorced, the order of benefits is:

. The plan of the custodial parent;
. The plan of the spouse of the custodial parent;
. The plan of the noncustodial parent; and then
. The plan of the spouse of the noncustodial parent.

(3) Active or inactive employee. The plan that covers a person as an employee who is neither laid off nor retired, is primary. The same would hold true if a person is a dependent of a person covered as a retiree and an employee. If the other plan does not have this rule, and if, as a result, the plans do not agree on the order of benefits, this rule is ignored. Coverage provided an individual as a retired worker and as a dependent of an actively working spouse will be determined under the rule labeled B(1).

(4) Continuation coverage. If a person whose coverage is provided under a right of continuation provided by federal or state law also is covered under another plan, the plan covering the person as an employee, member, subscriber or retiree (or as that person's dependent) is primary, and the continuation coverage is secondary. If the other plan does not have this rule, and if, as a result, the plans do not agree on the order of benefits, this rule is ignored.

(5) Longer or shorter length of coverage. The plan that covered the person as an employee, member, subscriber or retiree longer is primary.

(6) If the preceding rules do not determine the primary plan, the allowable expenses shall be shared equally between the plans meeting the definition of plan under this regulation. In addition, this plan will not pay more than it would have paid had it been primary.

EFFECT ON THE BENEFITS OF THIS PLAN

A. When this plan is secondary, it may reduce its benefits so that the total benefits paid or provided by all plans during a claim determination period are not more than 100 percent of total allowable expenses. The difference between the benefit payments that this plan would have paid had it been the primary plan, and the benefit payments that it actually paid or provided shall be recorded as a benefit reserve for the covered person and used by this plan to pay any allowable expenses, not otherwise paid during the claim determination period. As each claim is submitted, this plan will:

(1) Determine its obligation to pay or provide benefits under its contract;

(2) Determine whether a benefit reserve has been recorded for the covered person; and

(3) Determine whether there are any unpaid allowable expenses during that claims determination period.

If there is a benefit reserve, the secondary plan will use the covered person's benefit reserve to pay up to 100% of total allowable expenses incurred during the claim determination period. At the end of the claims determination period, the benefit reserve returns to zero. A new benefit reserve must be created for each new claim determination period.

B. If a covered person is enrolled in two or more closed panel plans and if, for any reason, including the provision of service by a non-panel provider, benefits are not payable by one closed panel plan, COB shall not apply between that plan and other closed panel plans.

RIGHT TO RECEIVE AND RELEASE NEEDED INFORMATION

Certain facts about health care coverage and services are needed to apply these COB rules and to determine benefits payable under this plan and other plans. [Organization responsibility for COB administration] may get the facts it needs from or give them to other organizations or persons for the purpose of applying these rules and determining benefits payable under this plan and other plans covering the person claiming benefits. [Organization responsibility for COB administration] need not tell, or get the consent of, any person to do this. Each person claiming benefits under this plan must give [Organization responsibility for COB administration] any facts it needs to apply those rules and determine benefits payable.

FACILITY OF PAYMENT

A payment made under another plan may include an amount that should have been paid under this plan. If it does,

[Organization responsibility for COB administration] may pay that amount to the organization that made that payment. That amount will then be treated as though it were a benefit paid under this plan. [Organization responsibility for COB administration] will not have to pay that amount again. The term "payment made" includes providing benefits in the form of services, in which case "payment made" means reasonable cash value of the benefits provided in the form of services.

RIGHT OF RECOVERY

If the amount of the payments made by [Organization responsibility for COB administration] is more than it should have paid under this COB provision, it may recover the excess from one or more of the persons it has paid or for whom it has paid; or any other person or organization that may be responsible for the benefits or services provided for the covered person. The "amount of the payments made" includes the reasonable cash value of any benefits provided in the form of services.

ATTACHMENT I

COT/GAD X-10 VENDOR ELECTRONIC FUNDS (RFT) REGISTRATION REQUEST FORM

State of Maryland
Comptroller of Maryland

Vendor Electronic Funds Transfer (EFT) Registration Request Form

Date of request _____

Business identification information (Address to be used in case of default to check):

Business name _____

Address line 1 _____

Address line 2 _____

City _____ State _____

Zip code ☐☐☐☐☐ ☐☐☐☐

Business taxpayer identification number:

Federal Employer Identification Number: ☐☐ ☐☐☐☐☐☐☐

(or) Social Security Number: ☐☐☐ ☐☐ ☐☐☐☐

Business contact name, title, and phone number including area code. (And address if different from above).

_____

_____

Financial institution information:

Name and address _____

_____

Contact name and phone number (include area code)

_____

ABA number ☐☐☐☐☐☐☐☐☐

Account number ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Account type ☐ Checking ☐ Money Market

A voided check from the bank account must be attached.

Transaction requested:

1. ☐ Initiate all disbursements via EFT to the above account.
2. ☐ Discontinue disbursements via EFT, effective _____
3. ☐ Change the bank account to above information – a copy of the approved Registration Form for the previous bank account must be attached.

(OVER)

I am authorized by *_____ (hereinafter Company) to make the representations contained in this paragraph. Company authorizes the Comptroller and the Treasurer of Maryland to register it for electronic funds transfer (EFT) using the information contained in this registration form. Company agrees to receive all funds from the State of Maryland by electronic funds transfer according to the terms of the EFT program. Company agrees to return to the State of Maryland any EFT payment incorrectly disbursed by the State of Maryland to the Company's account. Company agrees to hold harmless the State of Maryland and its agencies and departments for any delays or errors caused by inaccurate or outdated registration information or by the financial institution listed above.

*Name of registering business entity

_____

Signature of company treasurer, controller, or chief financial officer and date

Completed by GAD/STO

Date Received _____

GAD registration information verified _____ Date to STO_____

STO registration information verified _____ Date to GAD_____

R*STARS Vendor No. and Mail Code Assigned:

_____/_____/_____ _____

_____ _____

State Treasurer's Office approval date General Accounting Division approval date

_____

To Requestor:

Please retain a copy of this form for your records. Please allow approximately 30 days from the date of your request for the Comptroller's and Treasurer's Offices to process your request. Failure to maintain current information with this office could result in errors in payment processing. If you have any questions, please call the EFT registration desk at 410-260-7375.

Please submit form to: EFT Registration, General Accounting Division
Room 205, P.O. Box 746
Annapolis, Maryland 21404-0746

COT/GAD X-10

ATTACHMENT J-1

UTILIZATION REPORT INSTRUCTIONS

Attachments J-1a, J-1b and J-1c are reporting templates that outline for illustrative purposes only the minimum reporting requirements for the term of the Contract.

During the contract term, all quarterly and annual utilization reports must be accompanied by an executive summary which summarizes the reports, including but not limited to:

- An analysis of trends and utilization including highly utilized services
- Comparisons to normative benchmark data
- Analysis of network savings, and
- Analysis of utilization by State subgroups.

Attachment J-1a: Utilization and Cost Schedule

Complete the following exhibit for each plan type (DPPO and DHMO) and for each of the census subgroups (actives, satellites, direct pay, retirees, and total). Enter the number of members you assume in the space below.

Vendor: _____ **Plan type:** _____

Subgroup: _____ **Total Members:** _____

Service Category	Quarterly Results from mm/dd/yy through mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
In-Network - General Dentist									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
In-Network - Specialty Dentist									
Diagnostic (0100-0999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Quarterly Results from mm/dd/yy through mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Out-of-Network - General Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
Out-of-Network - Specialty Dentists									
Diagnostic (0100-0999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Quarterly Results from mm/dd/yy through mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Total – In-Network-General and Specialty Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
Total - Out-of-Network-General and Specialty Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Resotative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Quarterly Results from mm/dd/yy through mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Total - All Provider Types - In-Network and Out-of-Network									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Year to Date Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
In-Network - General Dentist									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
In-Network - Specialty Dentist									
Diagnostic (0100-0999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Year to Date Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Out-of-Network - General Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
Out-of-Network - Specialty Dentists									
Diagnostic (0100-0999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Year to Date Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Total – In-Network-General and Specialty Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
Total - Out-of-Network-General and Specialty Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Resotative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Year to Date Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Total - All Provider Types - In-Network and Out-of-Network									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Most Recent 12 Months ending: mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
In-Network - General Dentist									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
In-Network - Specialty Dentist									
Diagnostic (0100-0999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Most Recent 12 Months ending: mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Out-of-Network - General Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
Out-of-Network - Specialty Dentists									
Diagnostic (0100-0999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Most Recent 12 Months ending: mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Total – In-Network-General and Specialty Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									
Total - Out-of-Network-General and Specialty Dentists									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Resotative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

Attachment J-1a (cont.): Utilization and Cost Schedule

Vendor: _____

Subgroup: _____

Service Category	Most Recent 12 Months ending: mm/dd/yy Enter start date: Enter end date:								
						Unit Cost			
	No. of Services	Utilization Per 1,000	Discounted Charges or Value of Services	Benefits Paid by Plan	Benefits Paid by Member	Discounted Charges or Value of Services	Benefits Paid by Plan	Plan Paid PMPM	Member Paid PMPM
Total – All Provider Types - In-Network and Out-of-Network									
Diagnostic (0100-0999)									
Preventive (1000-1999)									
Restorative, Minor (2000-2399)									
Restorative, Major (2510-2999)									
Endodontics (3000-3999)									
Periodontics (4000-4999)									
Prosthodontics, Removable (5000-5899)									
Prosthodontics, Fixed (6200-6999)									
Oral Surgery (7000-7999)									
Orthodontics (8000-8999)									
Adjunctive General Services (9000-9999)									
Total									

ATTACHMENT J-1b: Membership Analysis

Vendor: _____

Membership by Plan Type and Subgroup							
	Number of Employees / Retirees	**Number of Members**	**Members Average Age**	**Members% Male**	**Members % Female**	**% Utilization**	**Paid Amount per Employee / Retiree per Month**
DPPO - Total							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DPPO - Actives							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DPPO - Direct Pay							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DPPO - Satellites							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DPPO - Retirees							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	

Membership by Plan Type and Subgroup							
	Number of Employees / Retirees	**Number of Members**	**Members Average Age**	**Members% Male**	**Members % Female**	**% Utilization**	**Paid Amount per Employee / Retiree per Month**
DHMO - Total							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DHMO - Actives							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DHMO - Direct Pay							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DHMO - Satellites							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	
DHMO - Retirees							
Prior Period				0.0%	0.0%	0.0%	
Current Period				0.0%	0.0%	0.0%	
Change				0.0%	0.0%	0.0%	

ATTACHMENT J-1c: DPPO Network Utilization (Geographic)

Vendor: _____

Subgroup: _____

Metropolitan/ Geographic Area (Subtotal by County)	Actives		Direct Pay		Satellites	
	% of Services Provided by In-Network Dentists	% of Benefits Paid by Plan to In-Network Dentists	% of Services Provided by In-Network Dentists	% of Benefits Paid by Plan to In-Network Dentists	% of Services Provided by In-Network Dentists	% of Benefits Paid by Plan to In-Network Dentists
Anne Arundel County						
Baltimore City						
Baltimore County						
Carroll County						
Harford County						
Howard County						
Central Maryland						
Caroline County						
Cecil County						
Dorchester County						
Kent County						
Queen Anne's County						
Somerset County						
Talbot County						
Wicomico County						
Worcester County						
Eastern Shore						
Calvert County						
Charles County						
St. Mary's County						
Southern Maryland						
District of Columbia						
Montgomery County						
Prince George's County						
Washington Metro						
Allegheny County						
Frederick County						
Garrett County						
Washington County						
Western Maryland						

ATTACHMENT J-1c (cont.): DPPO Network Utilization (Geographic)

Vendor: _____

Subgroup: _____

Metropolitan/ Geographic Area (Subtotal by County)	Retirees		Total	
	% of Services Provided by In-Network Dentists	% of Benefits Paid by Plan to In-Network Dentists	% of Services Provided by In-Network Dentists	% of Benefits Paid by Plan to In-Network Dentists
Anne Arundel County				
Baltimore City				
Baltimore County				
Carroll County				
Harford County				
Howard County				
Central Maryland				
Caroline County				
Cecil County				
Dorchester County				
Kent County				
Queen Anne's County				
Somerset County				
Talbot County				
Wicomico County				
Worcester County				
Eastern Shore				
Calvert County				
Charles County				
St. Mary's County				
Southern Maryland				
District of Columbia				
Montgomery County				
Prince George's County				
Washington Metro				
Allegheny County				
Frederick County				
Garrett County				
Washington County				
Western Maryland				

ATTACHMENT N

DENTAL PAYMENT PROCEDURE

All reports are generated by the State and forwarded to the vendor to support monthly payments as described below:

Active Employees: The State will send a payment to the vendor once a month. The first payment for the calendar year is paid in early February. This payment will provide an estimated payment for the months of January and February. The estimate is based on the first Central Payroll and University of Maryland deduction report for the month of January. The State will multiply this first payroll by four, thereby estimating two months worth of deductions. The next payment for the plan year will paid in March and will include reconciliation for January. The plan should receive this payment around March 15th.

Example:

Payment #1 - January & February Payment

First deduction report in January for Central payroll (CPB) employees	$500,000
for University of Md. (UOM)	$250,000
	$750,000

January estimated payment	2 x $750,000 =	$1,500,000
February " "	2 x $750,000 =	$1,500,000
Payment #1 of plan year		$3,000,000

Payment #2 – March Payment

Actual deductions for January CPB – P.P.E. 01/11/00		$500,000
P.P.E. 01/25/00	$550,000	
UOM–P.P.E. 01/15/00		$250,000
P.P.E. 01/29/00		$260,000
Total January actual deductions		$1,560,000
January estimated payment	2 x $750,000 =	$1,500,000
Adjustment for January		$60,000
March estimated payment	January actuals	$1,560,000
Payment #2 – March 15th		$1,620,000

Payment # 3 will adjust for February and provide an estimated payment for April.
Payments #4 through #12 will follow same procedure through the plan year.

These payments will also include any retroactive adjustments, No Pay payments or refund adjustments processed during the month.

Retirees: The State will send a payment to the vendor once a month. These payments are based on actual deduction reports from the State Retirement System. The first payment for the calendar year is paid in early February. Since pension and retirement checks are not processed until the end of the month, retiree deduction reports are not available until the first of the month following the period of coverage.

Payment #1 - January payment will be paid around the 15th of February based on the actual January retiree deduction report.

Payment #2 - February payment will be paid around the 15th of March based on the actual February retiree deduction report.

Payments #3 through #12 will follow the same procedure.

Retiree payments may also include any retroactive adjustments received during the month , along with any payments received on behalf of TIAA-CREF retirees and refund adjustments processed during the month.

Direct Pay Enrollees: This category includes those on COBRA, contractual employees, LAW injury and other individuals who are billed directly by the State for their health coverage. The State will send a payment to the vendor once a month. These payments are based on actual premiums received during a calendar month. The first payment for the calendar year is paid by the end of February.

This payment will include all premiums received during the month of January, regardless of the month premiums are being paid. For example, if the State receives a payment from an individual in January that pays for the months of January through April, the State will forward payment for the four months. A report detailing individuals for whom premiums have been received during the prior month will be forwarded to the vendor to support the monthly payment.

Payment #1 - January payment will be paid around the 25th of February based on the actual premiums received during the month of January.

Payment #2 - February payment will be paid around the 25th of March based on the actual premiums received during the month of January.

Payments #3 through #12 will follow the same procedure.

Satellite Employees: This category includes governmental and non-profit agencies covered by the State's program. The State will send a payment to the vendor once a month. These payments are based on actual premiums received during a calendar month. The first payment for the calendar year is paid in early February. This payment will include all premiums received during the month of January, regardless of the month premiums are being paid. For example, if the State receives a payment from an agency in January that pays for the months of January and February, the State will forward payment for the two months. A report detailing individuals for whom premiums have been received during the prior month will be forwarded to the vendor to support the monthly payment.

Payment #1 - January payment will be paid around the 15th of February based on the actual premiums received during the month of January.

Payment #2 - February payment will be paid around the 15th of March based on the actual premiums received during the month of January.

Payments #3 through #12 will follow the same procedure.